View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Electronic Thesis and Dissertation Archive - Università di Pisa

Università di Pisa

Facoltà di Scienze Matematiche Fisiche e Naturali

Corso di Laurea Specialistica in Matematica

Anno Accademico 2007/2008

Elaborato finale

IL PROBLEMA INVERSO DI GALOIS

Candidato
Vincenzo Luca Mantova

Relatore
Chiar.mo Prof.
Roberto Dvornicich

Controrelatore
Chiar.ma Prof.
Ilaria Del Corso

Indice

Introduzione

Il *problema inverso di Galois* è la domanda se esiste o no un'estensione di un campo dato avente gruppo di Galois assegnato. Mentre il problema classico di associare un gruppo ad ogni estensione algebrica è ampiamente risolto, il problema inverso è attualmente aperto. Il caso che andremo ad analizzare sarà quello in cui il campo base sarà $\mathbb{Q}$ e i gruppi saranno finiti. Molti dei risultati che otterremo saranno automaticamente validi anche su $\mathbb{Q}^{ab}$.

Il primo strumento di cui ci si avvale è il Teorema di Irriducibilità di Hilbert:

Teorema. *Per ogni polinomio $f(X,Y) \in \mathbb{Q}(X)[Y]$ irriducibile su $\mathbb{Q}(X)$ e di grado almeno 1 in Y, esistono infinite specializzazioni $X \mapsto b \in \mathbb{Q}$ per le quali $f(b,Y) \in \mathbb{Q}[Y]$ resta irriducibile su $\mathbb{Q}$.*

Il fatto interessante è che la specializzazione conserva, oltre all'irriducibilità, anche il gruppo di Galois del polinomio f, quando questo generi un'estensione normale. In tal modo possiamo studiare le estensioni di $\mathbb{Q}(t)$ piuttosto che le estensioni di $\mathbb{Q}$. Vedremo di questo teorema una dimostrazione facente uso di soli teoremi elementari di analisi complessa; in Appendice sarà trattata anche una dimostrazione basata sulla teoria dei modelli non standard.

Il secondo teorema che useremo è il Teorema di Esistenza di Riemann in forma profinita

Teorema. *Sia S un insieme finito di posti di $\mathbb{P}(\mathbb{C}(t)/\mathbb{C})$. Allora il gruppo di Galois dell'estensione algebrica massima N_S ramificata solo in S è*

$$\mathrm{Gal}(N_S/\mathbb{C}(t)) \cong \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = e \rangle^{\widehat{}}$$

con $s = |S|$.

I generatori γ_i sono generatori di gruppi di inerzia sopra i posti di S. Conseguenza immediata è che ogni gruppo finito che abbia s generatori $\sigma_1, \dots, \sigma_s$ che soddisfino $\sigma_1 \cdots \sigma_s = e$ si realizza su $\mathbb{C}(t)$. Vedremo come il Teorema di Esistenza di Riemann si può trasferire sui sottocampi algebricamente chiusi di $\mathbb{C}$, tra i quali ci interesserà $\overline{\mathbb{Q}}$.

Con i teoremi appena citati abbiamo quindi modo di conoscere la struttura del gruppo $\mathrm{Gal}(N_S/\overline{\mathbb{Q}}(t))$. Conoscere anche la struttura di $\mathrm{Gal}(N_S/\mathbb{Q}(t))$ ci permetterebbe di risolvere il problema inverso su $\mathbb{Q}$; tuttavia tale struttura non è ancora nota esplicitamente. Vedremo tuttavia che

$$\mathrm{Gal}(N_S/\mathbb{Q}(t)) \cong \mathrm{Gal}(N_S/\overline{\mathbb{Q}}(t)) \rtimes \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

L'azione del gruppo $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sul primo fattore si può esprimere in modo parzialmente esplicito tramite il carattere ciclotomico. Se assumiamo che il luogo di ramificazione S sia invariante per $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ otterremo che

$$[\gamma_i] = [\gamma_{i^\delta}^{c(\delta)}]$$

dove $[\gamma]$ è la classe di coniugio di γ in $\mathrm{Gal}(N_S/\overline{\mathbb{Q}}(t))$.

Ora le possibili scelte di s generatori per un gruppo G assegnato classificano completamente tutte le sottoestensioni di M_S con gruppo G; in particolare due sistemi di generatori inducono la stessa estensione se e soltanto se sono equivalenti per automorfismo di G. Tale classificazione è detta classificazione di Hurwitz. In particolare due sistemi di generatori coniugati in G inducono lo stesso sottocampo. Vedremo che l'estensione $N_{\boldsymbol{\sigma}}$ identificata da un particolare sistema di generatori $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_s)$ ha un campo minimale di definizione $K_{\boldsymbol{\sigma}}$ (sotto l'ipotesi che G abbia complementare per il centro), ovvero un sottocampo tale per cui esiste un $N'_{\boldsymbol{\sigma}}$ tale per cui $\mathrm{Gal}(N'_{\boldsymbol{\sigma}}/K_{\boldsymbol{\sigma}}) \cong \mathrm{Gal}(N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t))$. Il nostro scopo è dunque arrivare a mostrare che $K_{\boldsymbol{\sigma}} = \mathbb{Q}(t)$.

Studiando l'azione del carattere ciclotomico, nell'ipotesi che S sia invariante per $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, mostreremo allora che il campo $K_{\boldsymbol{\sigma}}$ deve necessariamente contenere un'estensione abeliana di $\mathbb{Q}$ dipendente solo dalle classi di coniugio dei generatori e da S. Tale campo sarà proprio $\mathbb{Q}$ nell'ipotesi, per esempio, che le classi di coniugio dei generatori siano *razionali*, ovvero tali per cui $C^m = C$ per ogni m che non divide $|G|$.

Per riuscire a dire che $K_{\boldsymbol{\sigma}} \cap \overline{\mathbb{Q}}$ coincide con l'estensione abeliana faremo allora uso della condizione di *rigidità*: si dirà rigido un vettore di classi $\mathbf{C} = (C_1, \ldots, C_s) \in \mathrm{Cl}(G)^s$ quando tutte le scelte di generatori $\sigma_i \in C_i$ soddisfacenti le proprietà prima citate saranno coniugate fra di loro in G. Quando tale condizione è soddisfatta, e il vettore $\mathbf{C}$ è anche di classi razionali, otterremo che è possibile realizzare il gruppo G su $\mathbb{Q}(t)$.

Il criterio di rigidità appena enunciato si può poi rapidamente generalizzare al caso in cui il vettore $\mathbf{C}$ non sia razionale, ma tale per cui $\mathbf{C}^m = (C_1^m, \ldots, C_s^m)$ sia di nuovo il vettore $\mathbf{C}$ con le componenti permutate. In tal caso vedremo come una scelta oculata del luogo di ramificazione S permette di ottenere nuovamente realizzazioni di G su $\mathbb{Q}(t)$. Ulteriori generalizzazioni si possono ottenere considerando il fatto che le sottoestensioni di indice finito di $\overline{\mathbb{Q}}(t)$ sono della forma $\overline{\mathbb{Q}}(\tilde{t})$; è possibile infatti in questo modo estendere la ricerca dei gruppi G oltre che in $\mathrm{Gal}(N_S/\overline{\mathbb{Q}}(t))$ anche in $\mathrm{Aut}(N_S/\overline{\mathbb{Q}})$. Potremo inoltre valutare la possibilità di realizzare simultaneamente il gruppo G, in questo caso specifico con centro banale, e un suo gruppo di automorfismi H considerando $G < H$; sotto opportune ipotesi sarà possibile ottenere un'estensione N tale per cui $\mathrm{Gal}(N/\mathbb{Q}(t')) \cong G$ e $\mathrm{Gal}(N/\mathbb{Q}(t'')) \cong H$, compatibilmente con l'immersione $G < H$.

Le realizzazioni ottenute con i criteri di rigidità possono poi essere unite l'una all'altra per ottenere gruppi più complessi. Vedremo come prodotti diretti ed alcuni tipi speciali di prodotto semidiretto, i prodotti a ghirlanda, saranno costruibili a patto di aver già realizzato i loro fattori. Vedremo anche, attraverso il concetto di realizzazione GAR, che è anche possibile costruire gruppi a partire dai loro fattori di composizione; in altre parole, se abbiamo

$\phi : G \to H$ un epimorfismo e H è un gruppo realizzato come $\mathrm{Gal}(K/\mathbb{Q})$, scopriremo che sotto opportune condizioni algebriche su $\ker(\phi)$ esisterà una sovraestensione $L \supset K$ con gruppo di Galois G su $\mathbb{Q}$ e tale per cui la restrizione a K fornirà proprio l'omomorfismo ϕ. Un criterio particolare di rigidità ci fornirà immediatamente dei gruppi con realizzazione GAR.

Infine vedremo degli esempi classici di applicazione dei criteri di rigidità; otterremo realizzazioni di S_n, di A_n e di $\mathrm{PSL}_2(p)$ (per $p \not\equiv \pm 1 (\mod 24)$) su $\mathbb{Q}$. Vedremo inoltre molto rapidamente come le tecniche di composizione dei gruppi possono essere eseguite in modo algoritmico, così da permettere la costruzione esplicita e induttiva di polinomi con gruppi di Galois assegnati.

Capitolo 1

Analisi e geometria

1.1 Campi hilbertiani

Definizione 1.1. Un campo k si dice *hilbertiano* se per ogni polinomio $f(x,y) \in k(x)[y]$ irriducibile rispetto a y esistono infiniti $b \in k$ per cui $f(b,y)$ è irriducibile in $k[y]$.

Tutti i campi hanno l'interessante proprietà di conservare, quando si conservi l'irriducibilità dei polinomi, i gruppi di Galois delle estensioni normali. Questo fatto è fondamentale per giustificare tutto lo studio che seguirà nelle prossime pagine.

Proposizione 1.2. *Sia k un campo (anche non hilbertiano), K un'estensione finita normale di $k(x)$ e $f(x,y)$ il polinomio minimo di un generatore dell'estensione. Allora per quasi tutti i $b \in k$ si ha che se $f(b,y)$ è irriducibile su $k[y]$, il campo $K' := k[y]/(f(b,y))$ è di Galois su k con gruppo di Galois isomorfo a $G := \mathrm{Gal}(K/k(x))$.*

Dimostrazione. Chiamiamo ω_b l'omomorfismo di specializzazione $k(x)[y] \to k[y]$. Tale mappa passa al quoziente per teorema di omomorfismo:

$$\begin{array}{ccc} k(x)[y] & \xrightarrow{\quad\omega_b\quad} & k[y] \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ K \cong k(x)[y]/(f(x,y)) & \xrightarrow{\overline{\omega}_b} & K' \cong k[y]/(f(b,y)) \end{array}$$

Ogni elemento di G agisce allora, tramite $\overline{\omega}_b$, come automorfismo di $G' := \mathrm{Gal}(K'/k)$, poiché $\omega_b(k(x)) = k$. Per valutarne l'iniettività, siano $\alpha_1, \ldots, \alpha_n$ le radici di $f(x,y)$ in K rispetto a y, in modo che sia $f(x,y) = (y-\alpha_1)\cdots(y-\alpha_n)$. Tali radici sono tutte distinte per irriducibilità di f come pure le loro immagini in K' per la stessa ragione su $\omega_b(f)$. Due automorfismi $\sigma, \sigma' \in G$ sono distinti quando differiscono su un generatore α_i, pertanto anche tramite $\overline{\omega}_b$ resteranno distinti.

Basta notare ora che i gradi delle estensioni sono uguali, quindi anche gli ordini di G e G', per concludere che $G \cong G'$. □

Per tutti i campi hilbertiani valgono le seguenti proprietà:

Proposizione 1.3. *Se k è hilbertiano, qualsiasi sua estensione finita l è hilbertiana.*

Inoltre gli infiniti b che rendono irriducibile un polinomio dato possono essere scelti in k.

Dimostrazione. Sia $h(x,y)$ un polinomio in $l(x)[y]$ irriducibile rispetto a y. Esso genera un'estensione $L := l(x)[y]/(h(x,y))$ di grado $\deg_y(h) \cdot [l : k]$ su k; sia $f(x,y)$ il polinomio minimo di un generatore di $L/k(x)$ e b un valore per cui esso resti irriducibile dopo l'applicazione di ω_b. Il campo $\overline{\omega}_b(L)$ è generato su $\overline{\omega}_b(l(x)) = l$ da una radice di $h(b,y)$, quindi confrontando i gradi deduciamo che $h(b,y)$ è irriducibile.

Per ipotesi di hilbertianità di k esistono infiniti b che rendono $f(b,y)$ irriducibile, pertanto ve ne sono infiniti anche per $h(x,y)$ ed appartengono a k. □

Proposizione 1.4. *Se k è hilbertiano, per qualunque famiglia finita di polinomi $p_1(x,y), \dots, p_n(x,y)$ irriducibili su $k(x)$ esistono infiniti $b \in k$ per cui le loro specializzazioni restano irriducibili.*

Dimostrazione. Prendiamo un'estensione K di $k(x)$ che contenga una radice per ognuno dei polinomi $p_i(x,y)$; sia $f(x,y)$ il polinomio minimo di un suo generatore. Analogamente alla proposizione precedente, per ogni b per cui $f(b,y)$ resta irriducibile il raffronto dei gradi delle estensioni garantisce che i $p_i(b,x)$ sono irriducibili anch'essi. Quindi esistono infiniti b che rendono irriducibili simultaneamente tutti i p_i. □

Quest'ultima proposizione ha una sorta di inverso che ci sarà molto utile per lo studio dell'hilbertianità di $\mathbb{Q}$.

Proposizione 1.5. *Se per qualsiasi famiglia finita di polinomi $p_1(x,y), \dots, p_n(x,y) \in k[x,y]$ irriducibili di grado maggiore di 1 in y esistono infiniti $b \in k$ per i quali nessun polinomio specializzato $p_i(b,y)$ ha radice in k, allora k è hilbertiano.*

Dimostrazione. Sia $f(x,y)$ un polinomio in $k[x,y]$ irriducibile su $k(x)$ di grado $n \geq 1$ in y. Nell'estensione da esso generata esso sarà il prodotto di monomi $(y - \alpha_i)$, tali per cui qualsiasi loro prodotto calcolato su un sottoinsieme proprio di indici $I \subset \{1, \dots, n\}$ non apparterrà a $k(x)[y]$; in particolare, ognuno di questi prodotti avrà un coefficiente $d_I(x) \notin k(x)$.

Siano $p_I(x,y)$ dei polinomi irriducibili a coefficienti in k che abbiano $d_I(x)$ come radici. Per ipotesi esistono infiniti b tali per cui le loro specializzazioni $p_I(b,y)$ non hanno radici in k. Pertanto, specializzando, vale che $\prod_{i \in I}(y - \overline{\omega}_b(\alpha_i)) \notin k(y)$, poiché uno dei suoi coefficienti sarà $d_I(b)$ che non apparterrà a k in quanto radice di $p_I(b,y)$. Allora $f(b,y)$ è irriducibile per infiniti b, e k è hilbertiano. □

Proposizione 1.6. *Se k è hilbertiano e $f(x_1, \dots, x_s)$ è un polinomio in $s \geq 2$ variabili irriducibile su k di grado almeno 1 in x_s, esistono infiniti b per i quali $f(b, x_2, \dots, x_s)$ sia irriducibile su k.*

Dimostrazione. Riduciamo il problema al caso in due variabili usando la specializzazione di Kronecker $S_d f(x,y) := f(x, y, y^d, \dots, y^{d^{s-2}})$. Scegliamo d intero

maggiore di tutti i gradi delle variabili x_i in f e scriviamo la fattorizzazione in irriducibili di $S_d f$:

$$S_d f(x,y) = g(x) \prod_i g_i(x,y).$$

Vi sono infiniti b per cui tutti i g_i restano irriducibili per la proposizione 1.4; imponiamo anche che valga $g(b) \neq 0$. Supponiamo ora che sia $f(b, x_2, \dots, x_s) = h_1(x_2, \dots, x_s)h_2(x_2, \dots, x_s)$. Le relative specializzazioni $S_d h_1(y)$ e $S_d h_2(y)$ saranno prodotti di fattori $g_i(b,y)$ più un eventuale costante, per cui costruiamo $H_1(x,y)$ e $H_2(x,y)$ come prodotto dei fattori g_i corrispondenti. In tal modo $S_d f(x,y) = g(x)H_1(x,y)H_2(x,y)$.

Scriviamo per ogni monomio $x^k y^l$ l'espansione in base d di l; da essa otteniamo due polinomi $\tilde{h}_1(x_1, \dots, x_s)$, $\tilde{h}_2(x_1, \dots, x_s)$ per cui $S_d \tilde{h}_1 = gH_1$ e $S_d \tilde{h}_2 = gH_2$. Tali polinomi sono gli unici a soddisfare tali condizioni con gradi in $x_2, \dots, x_s$ tutti minori di d. Se il grado massimo di $\tilde{f} := \tilde{h}_1 \tilde{h}_2$ nelle varie variabili fosse minore di d, avremmo per unicità dell'espansione in base d che $f = \tilde{f}$, contro l'ipotesi di irriducibilità.

Osserviamo ora che gli $\tilde{h}_i(b, x_2, \dots, x_s)$ sono multipli scalari di $h_i(x_2, \dots, x_s)$, poiché hanno gradi limitati da $d-1$ e la stessa specializzazione di Kronecker a meno di costante. Questo implica che $\tilde{f}(b, x_2, \dots, x_s)$ è un multiplo scalare di $f(b, x_2, \dots, x_s)$. Il polinomio $\tilde{f}$ contiene però un monomio $c(x) x_2^{i_2} \cdots x_s^{i_s}$ con almeno un $i_v \geq d$, pertanto deve valere $c(b) = 0$. Questo può accadere in al più un numero finito di casi, per cui per i restanti infiniti b $f(b, x_2, \dots, x_s)$ deve essere irriducibile. □

Corollario 1.7. *Ogni estensione finitamente generata di un campo hilbertiano k è hilbertiana.*

Inoltre gli infiniti b che rendono irriducibile un polinomio dato possono essere scelti in k.

Dimostrazione. Sia $K := k(t_1, \dots, t_s)$ un'estensione di k puramente trascendente. Se $f(x, t_1, \dots, t_s, y)$ è un polinomio irriducibile in $k[x, t_1, \dots, t_s, y]$ esso è irriducibile anche in $K[x,y]$. Esistono infiniti $b \in k$ per i quali $f(x, t_1, \dots, t_s, y)$ è irriducibile in $K[y]$ per la proposizione 1.6, pertanto K è hilbertiano. Ora per la proposizione 1.3 ogni sua estensione finita è hilbertiana, con la proprietà che i valori b possono essere scelti in k, da cui la tesi. □

Abbiamo ora gli strumenti per dedurre la proprietà fondamentale che ci interessa dei campi hilbertiani.

Teorema 1.8. *Se k è hilbertiano, ogni gruppo di Galois che si realizza su $k(x_1, \dots, x_s)$, con $x_1, \dots, x_s$ algebricamente indipendenti su k, si realizza anche su k.*

Dimostrazione. Sappiamo che $G \cong \mathrm{Gal}(K/k(x_1, \dots, x_s))$. Basta applicare induttivamente il corollario 1.7 a $k(x_1, \dots, x_{s-1})(x_s)$ per far calare il grado di trascendenza su k, mentre ad ogni passo la proposizione 1.2 ci garantisce la conservazione del gruppo di Galois. □

Possiamo dire di più. Diamo prima due definizioni e un lemma algebrico.

Definizione 1.9. Un'estensione K di k si dice *regolare* se è un'estensione finitamente generata di k con la proprietà che k sia algebricamente chiuso in K ($\bar{k} \cap K = k$).

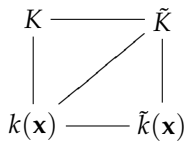
Diremo anche che L/K è *regolare* nel caso di estensioni finitamente generate su k se $\bar{k} \cap K = \bar{k} \cap L$.

Definizione 1.10. Si dice che un gruppo G *occorre regolarmente su* k, oppure che *ha una* G*-realizzazione su* k, se esiste un'estensione regolare K algebrica e normale su $k(\mathbf{x})$, con $\mathbf{x}$ vettore finito di variabili algebricamente indipendenti su k, per cui $G \cong \mathrm{Gal}(K/k(\mathbf{x}))$.

Lemma 1.11. *Sia K un'estensione di k finita su $k(\mathbf{x})$, dove $\mathbf{x}$ è un vettore finito di variabili algebricamente indipendenti su k, e sia $f(\mathbf{x}, y) \in k(\mathbf{x})[y]$ il polinomio minimo di un generatore dell'estensione. Allora K è regolare su k se e soltanto se f è irriducibile in $\bar{k}(\mathbf{x})$.*

Dimostrazione. Sia $\tilde{k}$ la chiusura algebrica di k in K. Se $\tilde{k} \neq k$ allora $[K : \tilde{k}] < [K : k]$, pertanto il polinomio $f(\mathbf{x}, y)$ che genera l'estensione non è irriducibile su $\tilde{k}(\mathbf{x})$.

Viceversa sia $\tilde{k}$ un'estensione finita di k. Sia allora $\tilde{K}$ il composto di $\tilde{k}$ e K in una chiusura algebrica di $k(\mathbf{x})$, e si intersechi K con $\tilde{k}(\mathbf{x})$; il campo risultante sarà necessariamente $k(\mathbf{x})$. Si deve allora avere che $[\tilde{K} : \tilde{k}] = [K : k]$, dunque il polinomio del generatore dell'estensione deve restare irriducibile. Per arbitrarietà di $\tilde{k}$, f resta irriducibile in $\bar{k}$. □



Teorema 1.12. *Se un gruppo G ha una G-realizzazione su k, ha anche una G-realizzazione su ogni sua estensione finita k'.*

Dimostrazione. Sia $K/k(\mathbf{x})$ una realizzazione geometrica di G. Sia $f(\mathbf{x}, y)$ il polinomio minimo di un generatore dell'estensione; tale polinomio resta irriducibile anche in una qualsiasi estensione k' algebrica su k, in particolare quando è finita. Allora il polinomio definisce un'estensione $K' := k'(\mathbf{x})[y]/(f(\mathbf{x}, y))$ per cui $[K' : k'(\mathbf{x})] = [K : k(\mathbf{x})]$.

Essendo $K \cap k' = k$ per ipotesi di regolarità, abbiamo $K' = k'K$, per cui K' è di Galois su $k'(\mathbf{x})$ e il suo gruppo, per proprietà delle torri, è isomorfo a $\mathrm{Gal}(K/k(\mathbf{x}))$. □

Vediamo ora un teorema più complesso dei precedenti, che ci consente di estendere l'hilbertianità di k ad alcune estensioni algebriche anche non finitamente generate.

Lemma 1.13. *Sia k hilbertiano e l/k una sua estensione finita. Siano $\pi, \tilde{\pi} \in l[x_1, x_2][y]$ monici in y, con x_1 e x_2 algebricamente indipendenti su l. Supponiamo che π non abbia radici in un campo di spezzamento di $\tilde{\pi}$; allora esistono infiniti $b_1, b_2 \in k$ per i quali la specializzazione $\pi(b_1, b_2, y)$ non abbia radici in un campo di spezzamento di $\tilde{\pi}(b_1, b_2, y)$.*

Dimostrazione. Sia $K/l(x_1, x_2)$ un'estensione di Galois finita contenente le radici di π e $\tilde{\pi}$. Essa sarà generata da un α con polinomio minimo $f(y) = f(x_1, x_2, y)$,

monico in y, a coefficienti in $l[x_1, x_2]$. La proposizione 1.7 ci garantisce che possiamo trovare infiniti b_1, b_2 in k per cui $f(b_1, b_2, y)$ sia irriducibile su l.

Senza perdere di generalità, supponiamo che π e $\tilde{\pi}$ siano polinomi separabili (modificando π e $\tilde{\pi}$ tramite l'eliminazione dei fattori irriducibili ripetuti sono ancora verificate le ipotesi e non cambia l'insieme delle radici nemmeno via specializzazione). Solo per un numero finito di specializzazioni di x_1 i discriminanti diventano nulli; per ognuna delle restanti specializzazioni solo un numero finito di scelte di b_2 annullano i discriminanti. Pertanto possiamo supporre che le specializzazioni di π e $\tilde{\pi}$ restino separabili.

A questo punto basta sfruttare l'azione di $\mathrm{Gal}(K/l(x_1, x_2))$ sulle radici dei due polinomi. Per l'ipotesi sui campi di spezzamento, esiste un omomomrfismo σ che fissa le radici di π ma permuta le radici di $\tilde{\pi}$; grazie alla proposizione 1.2 sappiamo che la stessa cosa accade quindi nel campo specializzato, di conseguenza le radici di $\pi(b_1, b_2, y)$ non possono essere contenute nel campo di spezzamento di $\tilde{\pi}(b_1, b_2, y)$. □

Teorema 1.14 (Weissauer)**.** *Sia k un campo hilbertiano e N una sua estensione di Galois (anche infinita). Sia M un'estensione propria finita di N. Allora M è hilbertiana.*

Inoltre i valori che rendono irriducibili un polinomio possono essere scelti in $k(\theta)$, dove θ è un generatore di N su M.

Dimostrazione. Come fatto per $\mathbb{Q}$, verificheremo che ogni famiglia finita di polinomi $p_i(x, y) \in M[x, y]$ irriducibili su $M(x)$ e di grado maggiore di 1 in y esistono infiniti $b \in M$ per cui le specializzazioni non hanno radici in M.

Prendiamo allora una famiglia finita di polinomi p_i come appena detto, e supponiamo che siano tutti monici escludendo il numero finito di possibili specializzazioni di x che annullino il coefficiente di grado massimo di qualche p_i. Supponendo anche che siano distinti, definiamo $p(x, y) := \prod_i p_i(x, y)$, che sarà un polinomio separabile. Nostro obiettivo ora è dimostrare che esistono infiniti $b \in M$ per i quali $p(b, y)$ non ha radici in M.

Dimostriamo innanzitutto che i fattori con radici in $\overline{M}(x)$ sono trascurabili. Se così fosse per un polinomio $p_j(x, y)$, essendo $\overline{M}(x)$ normale su $M(x)$ avremmo la fattorizzazione $p_j(x, y) = \prod_k (y - g_k(x))$. Per ogni $b \in M$ tale che $g_k(b) \in M$ abbiamo $g_k^\sigma(b) = g_k(b)$ per ogni $\sigma \in \mathrm{Gal}(\overline{M}(x)/M(x))$, per tanto se tali b fossero infiniti avremmo $g_k^\beta = g_k$ e quindi $g_k \in M(x)$, contro l'ipotesi di irriducibilità. Quindi i fattori p_j con una radice in $\overline{M}(x)$ hanno polinomi senza radici in M per quasi tutte le specializzazioni, per cui li trascuriamo dal prodotto $p(x, y)$.

Sia ora $M = N(\theta)$. Immaginando M immerso in una chiusura algebrica di k costruiamo l'estensione finita l di k aggiungendo i coefficienti di $p(x, y)$ e θ e facendo la chiusura normale. Chiamiamo $\tilde{k} := N \cap l$ e, dato che $\theta \notin \tilde{k}$, fissiamo un $\tilde{\theta} \in l$ coniugato non banale di θ su $\tilde{k}$. Consideriamo ora i polinomi $\pi(y) := p(x_1 + \theta x_2, y)$ e $\tilde{\pi}(y) := p(x_1 + \tilde{\theta} x_2, y)$ come polinomi a coefficienti in $l(x_1, x_2)$, dove x_1, x_2 sono algebricamente indipendenti su l.

Poniamo $t = x_1 + \theta x_2$, $\tilde{t} = x_1 + \tilde{\theta} x_2$. Abbiamo $l(x_1, x_2) = l(t, \tilde{t})$, e t è trascendente su $l(\tilde{t})$. Il polinomio $\pi(y) = p(t, y) \in l[t, y]$ non ha radici in $\bar{l}(t)$

per quanto affermato in precedenza, pertanto tutti i suoi fattori irriducibili hanno grado maggiore di 1.

Sia $\tilde{L}$ il campo di spezzamento di $\tilde{\pi}(y)$ su $\bar{l}(\tilde{t})$. Dato che t è trascendente su $\bar{l}(\tilde{t})$, quindi anche su $\tilde{L}$, i fattori irriducibili di $\pi(y)$ restano irriducibili; $\tilde{L}(t)$ contiene però tutte le radici di $\tilde{\pi}(y)$ e $l(x_1, x_2)$, pertanto contiene il campo di spezzamento di $\tilde{\pi}$ su $l(x_1, x_2)$. Quindi π non ha radici nel campo di spezzamento di $\tilde{\pi}$.

Chiamiamo ora $\tilde{M}$ il composto di N e l; è normale su k in quanto composizione di due estensioni normali. Fissiamo ora $\pi_{b_1 b_2}(y) := \pi(b_1 + b_2\theta, y)$ e $\tilde{\pi}_{b_1 b_2}(y) := \tilde{\pi}(b_1 + b_2\tilde{\theta}, y)$. Prendiamo l'intersezione del campo di spezzamento di $\pi_{b_1 b_2}$ con $\tilde{M}$, e chiamiamolo S; esso sarà generato dalle radici di $\pi_{b_1 b_2}$ contenute in $\tilde{M}$. $S \cap N$ è un'estensione normale di $\tilde{k}$, poiché ogni automorfismo di $N/\tilde{k}$ si estende ad un automorfismo di $\tilde{M}/\tilde{k}$ che lascia fisso l per costruzione di $\tilde{k}$ e pertanto lascia S invariato. Di conseguenza $S = (S \cap N)l$ è normale su $\tilde{k}$, quindi esiste un suo automorfismo che lascia invariato $\tilde{k}$ e che manda θ in $\tilde{\theta}$ (per costruzione di θ). Applicatolo alle radice di $\pi_{b_1 b_2}$ le manda in radici di $\tilde{\pi}_{b_1 b_2}$, quindi il campo di spezzamento di $\pi_{b_1 b_2}$ su l è contenuto nel campo di spezzamento di $\tilde{\pi}_{b_1 b_2}$.

Applichiamo infine il lemma 1.13 ai polinomi π e $\tilde{\pi}$; esistono infiniti b_1, b_2 in k per i quali $\pi_{b_1 b_2}$ non ha radici nel campo di spezzamento di $\tilde{\pi}_{b_1 b_2}$. Questo implica allora che $\pi_{b_1 b_2}$ non ha radici in $\tilde{M}$, ovvero nemmeno in M. Dato che $b_1 + \theta b_2$ sono tutti distinti, poiché $\theta \notin k$, otteniamo infiniti valori $b \in k(\theta)$ per cui $p(x, y)$ non ha radici. Quindi M è hilbertiano, e i valori b hanno la proprietà richiesta. □

Dal teorema appena enunciato possiamo dedurre il seguente teorema.

Teorema 1.15. *Sia k hilbertiano. Se un gruppo G occorre regolarmente su k, allora per ogni $m \geq 1$ esiste un'estensione di Galois di $k(x_1, \ldots, x_m)$ regolare su k con gruppo isomorfo a G.*

Dimostrazione. Data una realizzazione $K/k(x_1, \ldots, x_n)$, è semplice aumentare il numero di variabili aggiungendone di nuove algebricamente indipendenti dalle precedenti. La regolarità è evidentemente conservata come pure il gruppo di Galois. Sia $f(y)$ il polinomio minimo di un generatore dell'estensione, e supponiamo per semplicità che sia monico e a coefficienti in $k[x_1, \ldots, x_n]$.

Per diminuire il numero di variabili prendiamo il campo $\kappa = k(x_1^2, \ldots, x_{n-1})$, $N = \bar{k}(x_1^2, \ldots, x_{n-1})$ e $M = \bar{k}(x_1, \ldots, x_{n-1})$. Vale $M = N(x_1)$. Applicando il teorema 1.14 abbiamo che M è hilbertiano, e i valori b possono essere scelti in $k(x_1)$.

Per ipotesi di regolarità $f(y)$ è irriducibile anche su $M(x_n)$ (proposizione 1.11). Allora esistono infiniti $b \in k(x_1)$ che rendono la sua specializzazione $f(x_1, \ldots, x_{n-1}, b, y)$ irriducibile su M e a coefficienti in $k(x_1, \ldots, x_{n-1})$. L'estensione da esso generata su $k(x_1, \ldots, x_{m-1})$ è quindi regolare e il suo gruppo di Galois è ancora G per la proposizione 1.2. □

1.2 Teorema di Irriducibilità di Hilbert

Affrontiamo ora una dimostrazione analitica del fatto che $\mathbb{Q}$ e $\mathbb{Q}^{ab}$ siano hilbertiani; lo saranno di conseguenza, per la proposizione 1.3, tutti i campi di numeri. Partiamo da un classico risultato di analisi, il teorema della funzione implicita in versione analitica.

Proposizione 1.16. *Sia $p(z,x)$ un polinomio in x di grado n a coefficienti olomorfi in z. Se in un punto z_0 il polinomio è separabile, allora esiste un intorno V di z_0 nel quale esistono n funzioni $\psi_1,\dots,\psi_n$ tali che $p(z,\psi_i(z))=0$ identicamente su V.*

Dimostrazione. Sia x_i una radice di $p(z_0,x)$ e ε un valore tale per cui non ci siano radici nemmeno per $|x-x_i|\leq\varepsilon$. Allora, per continuità, possiamo scegliere δ in modo che per $|z-z_0|<\delta$ non ci siano zeri per $|x-x_i|=\varepsilon$. Usiamo ora l'integrale logaritmico per contare gli zeri fissato z:

$$n(z)=\frac{1}{2\pi\imath}\oint_{|x-x_i|=\varepsilon}\frac{p_x(z,x)}{p(z,x)}.$$

Per la scelta di δ la dipendenza da z è olomorfa, quindi $n(z)$ è costantemente 1 nell'intervallo scelto. Possiamo quindi calcolare

$$\phi_i(z)=\frac{1}{2\pi\imath}\oint_{|x-x_i|=\varepsilon}x\frac{p_x(z,x)}{p(z,x)}$$

che per il teorema del residuo sarà proprio lo zero del polinomio. Di nuovo la dipendenza è olomorfa, quindi ϕ_i è una funzione olomorfa tale che $p(z,\phi_i(z))=0$ e $\phi_i(z_0)=x_i$. □

Il nostro scopo sarà ora controllare il comportamento delle funzioni ψ_i per dedurre che $\mathbb{Q}$ è hilbertiano. Fissiamo innanzitutto un teorema del valor medio generalizzato.

Lemma 1.17. *Siano $s_0<s_1<\ldots<s_m$ numeri reali con $m\geq 1$. Sia $\phi(s)$ una funzione a valori reali definita nell'intervallo $[s_0,s_m]$ e con derivate continue fino all'ordine m. Sia V_m il determinante di Vandermonde:*

$$V_m=\begin{vmatrix}1 & s_0 & s_0^2 & \cdots & s_0^m\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & s_m & s_m^2 & \cdots & s_m^m\end{vmatrix}=\prod_{i>j}(s_i-s_j)$$

Allora esiste un numero σ in (s_0,s_m) per cui si abbia:

$$\frac{\phi^{(m)}(\sigma)}{m!}=\frac{1}{V_m}\begin{vmatrix}1 & s_0 & s_0^2 & \cdots & s_0^{m-1} & \phi(s_0)\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & s_m & s_m^2 & \cdots & s_m^{m-1} & \phi(s_m)\end{vmatrix}.$$

Dimostrazione. Definiamo la funzione $F(s)$:

$$F(s)=\begin{vmatrix}1 & s_0 & s_0^2 & \cdots & s_0^{m-1} & \phi(s_0)\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & s & s^2 & \cdots & s^{m-1} & \phi(s)\end{vmatrix}.$$

Chiamiamo c il valore

$$c = \frac{F(s_m)}{(s_m - s_0)\cdots(s_m - s_{m-1})}$$

e $G(s)$ la funzione

$$G(s) = F(s) - c(s - s_0)\cdots(s - s_{m-1}).$$

La funzione $G(s)$ si annulla in tutti i punti s_i, pertanto applicando ripetutamente il teorema del valor medio si ha $G^{(m)}(\sigma) = 0$ per qualche σ compreso fra s_0 e s_m. Esplicitando la derivata di $G(s)$:

$$G^{(m)}(\sigma) = F^{(m)}(\sigma) - m!c = 0.$$

D'altra parte possiamo espandere l'espressione di $F(s)$

$$F(s) = \sum_{i=0}^{m-1} c_i s^i + V_{m-1}\phi(s)$$

dove i c_i sono costanti determinate da $s_0, \ldots, s_m$. Derivando esplicitamente:

$$F^{(m)}(\sigma) = V_{m-1}\phi^{(m)}(\sigma).$$

In conclusione:

$$\frac{\phi^{(m)}(\sigma)}{m!} = \frac{c}{V_{m-1}} = \frac{F(s_m)}{(s_m - s_0)\cdots(s_m - s_{m-1})V_{m-1}} = \frac{F(s_m)}{V_m}.$$

□

Diamo anche la seguente definizione:

Definizione 1.18. Un insieme $M \subset \mathbb{N}$ si dice *sparso* se esiste un numero reale α con $0 < \alpha < 1$ per cui si abbia

$$|M \cap \{1, \ldots, n\}| \leq n^\alpha$$

per quasi tutti gli $n \in \mathbb{N}$.

Osservazione 1.19. L'unione finita di insiemi sparsi è sparsa e gli insiemi finiti sono sparsi.

Usiamo ora il lemma appena dimostrato per ricavare il seguente teorema:

Teorema 1.20. *Sia $\varphi(t)$ una funzione meromorfa in un intorno di 0. Sia $B(\varphi)$ l'insieme dei $b \in \mathbb{N}$ per i quali $\varphi(1/b)$ sia definito e intero. Allora $B(\varphi)$ è un insieme sparso a meno che φ non sia della forma $p(t)/t^k$ con $p(t) \in \mathbb{C}[t]$.*

Dimostrazione. Supponiamo che φ non sia della forma $p(t)/t^k$ e che $B(\varphi)$ non sia finito. Sviluppiamo allora la funzione φ come serie di Laurent in 0.

$$\varphi(t) = \sum_{i=k}^{\infty} a_i t^i.$$

I suoi coefficienti non sono quasi tutti nulli, e sono tutti reali, poiché $\varphi(t) = \overline{\varphi}(t)$ su $1/B(\varphi)$, che è un insieme che si addensa sull'origine.

$$\phi(s) = \varphi(s^{-1}) = \sum_{i=k}^{\infty} a_i s^{-i}.$$

Prendiamo ora una successione $s_0, \ldots, s_m$ crescente di interi per i quali $\phi(s_i) \in \mathbb{Z}$. Supponiamo m sufficientemente grande perché la serie

$$\phi^{(m)}(s) = \sum_{i=\mu}^{\infty} d_i s^{-i}$$

abbia sole potenze negative e poniamo μ in modo che sia $d_\mu \neq 0$. Allora $s^\mu \phi^{(m)}(s)$ tende a d_μ per s che va a infinito; pertanto esiste un $S > 0$ tale per cui $0 < |s^\mu \phi^{(m)}(s)| < |2d_\mu|$ per $s \geq S$.

Supponiamo ora che sia $s_0 > S$. Prendiamo σ come nel lemma 1.17; poiché tutti i valori nella matrice sono interi, $\frac{V_m \phi^{(m)}(\sigma)}{m!}$ è intero non nullo di modulo maggiore di 1. Ricaviamo quindi

$$(s_m - s_0)^{(m+1)(m+2)/2} \geq V_m \geq \frac{1}{|\phi^{(m)}(\sigma)|} \geq \frac{1}{|2d_\mu|}\sigma^\mu \geq \frac{1}{|2d_\mu|} s_0^\mu.$$

Prendendo $\lambda = 2\mu/(m+1)(m+2)$ otteniamo che

$$s_m - s_0 \geq s_0^\lambda.$$

L'insieme $B(\varphi)$ può ora essere scritto come unione di un insieme finito di interi minori di S_m e di m insiemi infiniti sui quali vale $b - a \geq a^\lambda$ tra due elementi successivi. Sia B uno di questi insiemi con tale proprietà.

Sia n un intero qualsiasi, e sia n' il numero di $b \in B$ per cui $\sqrt{n} < b \leq n$. Ogni b fra questi soddisfa la diseguaglianza $b - \sqrt{n} \geq \sqrt{n}^\lambda$, quindi vale $(n' - 1) \leq n^{1-\lambda/2}$. Ricaviamo quindi:

$$|B \cap \{1, \ldots, n\}| \leq \sqrt{n} + n' \leq \sqrt{n} + n^{1-\lambda/2} + 1$$

che implica evidentemente che B è sparso. Di conseguenza anche $B(\phi)$ è sparso. □

Applichiamo ora il teorema appena dimostrato alle radici di un polinomio irriducibile a coefficienti in $\mathbb{Q}$.

Lemma 1.21. *Sia $p(x, y) \in \mathbb{Q}[x, y]$ irriducibile su $\mathbb{Q}(x)$ e di grado $n > 1$ in y. Allora per quasi tutti gli $x_0 \in \mathbb{Z}$ valgono le seguenti:*

(a) Esiste un $\varepsilon > 0$ e n funzioni olomorfe $\psi_1(t), \ldots, \psi_n(t)$ definite per $|t| < \varepsilon$ tali che siano le radici di $p(x_0 + t, y) \in \mathbb{Q}[y]$.

(b) Se una $\psi_i(t)$ è una funzione razionale di t, esistono solo un numero finito di $q \in \mathbb{Q}$ per cui $\psi_i(q) \in \mathbb{Q}$.

(c) Sia $B(p, x_0)$ l'insieme dei $b \in \mathbb{N}$ per i quali $p(x_0 + 1/b, c) = 0$ per qualche $c \in \mathbb{Q}$. Allora $B(p, x_0)$ è sparso.

Dimostrazione. (a) Il polinomio $p(x,y)$ è irriducibile su $\mathbb{Q}(x)$, pertanto è separabile e il suo discriminante $D(x)$ è non nullo. Esistono allora soltanto un numero finito di b per i quali $p(b,y)$ non è separabile; escludendo questi possiamo allora applicare la proposizione 1.16 e ottenere le funzioni $\psi_i(t)$ desiderate.

(b) Supponiamo ora che $\psi := \psi_i$ sia una funzione razionale di t. Allora la funzione $p(x_0+t,\psi(t))$ è identicamente nulla come funzione razionale in t, ovvero $p(x_0+x,\psi(x))$ è nullo in $\mathbb{C}(x)$. L'elemento $\psi(x)$ è quindi algebrico su $\mathbb{Q}(x)$, ma dato che $\mathbb{C}(x)\cap\overline{\mathbb{Q}(x)} = \overline{\mathbb{Q}}(x)$ otteniamo che i coefficienti di $\psi(t)$ sono algebrici su $\mathbb{Q}$. Per ogni automorfismo σ di $\overline{\mathbb{Q}}/\mathbb{Q}$, $\psi^\sigma(q) = \psi(q)$ quando $q \in \mathbb{Q}$ e $\psi(q) \in \mathbb{Q}$. Se l'insieme dei q possibili è infinito allora vale sempre $\psi^\sigma = \psi$, quindi $\psi(x) \in \mathbb{Q}(x)$ è uno zero di $p(x,y)$ su $\mathbb{Q}(x)$. Dato però che p ha grado maggiore di 1 in y ed è irriducibile questo è assurdo.

(c) Moltiplicando per una costante in $\mathbb{Q}$ possiamo supporre p a coefficienti interi. Scriviamo

$$p(x,y) = \sum_{i=0}^{n} p_i(x)y^i$$

con $p_i(x) \in \mathbb{Z}[x]$. Prendendo N maggiore dei gradi dei $p_i(x)$ otteniamo

$$x^N p\left(x_0+\frac{1}{x},y\right) = \sum_{i=0}^{n} x^N p_i\left(x_0+\frac{1}{x}\right)y^i = \sum_{i=0}^{n} p_i'(x)y^i$$

con coefficienti interi. Ponendo $z = p_n'(x)y$ e moltiplicando tutto per $p_n'(x)^{n-1}$ otteniamo un polinomio $p'(x,z)$ monico in z a coefficienti interi:

$$p'(x,z) = z^n + \sum_{i=0}^{n-1} p_i'(x)p_n'(x)^{n-i-1}z^i.$$

Ora se $p(x_0+1/b,c) = 0$ per $c \in \mathbb{Q}$ e $b \in \mathbb{Z}$ abbiamo $p'(b,p_n'(b)c) = 0$; questo implica che $p_n'(b)c$ è intero su $\mathbb{Z}$, quindi intero in quanto razionale. Inoltre per qualche i, e se b è sufficientemente grande, vale $c = \psi_i(1/b)$.

Definiamo allora $\phi_i(t) = p_n'(t^{-1})\psi_i(t)$. Allora $b \in B(p,x_0)$ e $1/b < \varepsilon$ implicano che $\phi_i(1/b) \in \mathbb{Z}$ per qualche i. Di conseguenza escludendo un numero finito di elementi $B(p,x_0)$ è contenuto negli $B(\phi_i)$. Quando ϕ_i è una funzione razionale, il punto (b) ci garantisce che $B(\phi_i)$ è finito; altrimenti applichiamo il teorema 1.20 e otteniamo che $B(\phi_i)$ è sparso. Quindi $B(p,x_0)$ è sparso per quasi tutti gli $x_0 \in \mathbb{Z}$. □

Teorema 1.22 (Irriducibilità di Hilbert)**.** $\mathbb{Q}$ *è hilbertiano.*

Dimostrazione. Per la proposizione 1.5 ci basta verificare che per qualunque famiglia di polinomi $p_i(x,y) \in \mathbb{Q}[x,y]$ irriducibili su $\mathbb{Q}(x)$ e di grado maggiore di 1, esistono infiniti b per i quali le specializzazioni non hanno radice in $\mathbb{Q}$.

Siano allora $p_i(x,y)$ polinomi del tipo richiesto. Esisterà certamente un x_0 per i quali si applica il lemma 1.21 simultaneamente su tutti i polinomi. Sia C l'insieme dei $b \in \mathbb{N}$ tali per cui nessun polinomio $p_i(x_0+1/b,y)$ ha radice in $\mathbb{Q}$. Il suo complementare è l'unione dei $B(p_j,x_0)$, pertanto è sparso e C è infinito. □

Teorema 1.23. $\mathbb{Q}^{\mathrm{ab}}$ *è hilbertiano.*

Dimostrazione. $\mathbb{Q}^{ab}$ può essere scritto come estensione di $N := \mathbb{Q}^{ab} \cap \mathbb{R}$ semplicemente come $N[\imath]$. N è un'estensione normale di $\mathbb{Q}$ poiché $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ è abeliano, quindi qualunque sottogruppo, e pertanto qualunque sottoestensione, è normale. Possiamo allora applicare il 1.14 e dedurre che $\mathbb{Q}^{ab}$ è hilbertiano. □

1.3 Teorema di Esistenza di Riemann

Daremo per scontato il risultato seguente:

Teorema 1.24. *Sia $\mathcal{X}$ una superficie di Riemann compatta e $\mathcal{P} \in \mathcal{X}$. Allora esiste una funzione meromorfa su $\mathcal{X}$ che ha un polo in $\mathcal{P}$ e olomorfa su $\mathcal{X} \setminus \{\mathcal{P}\}$.*

Per una dimostrazione compatta si veda [9, Cor. 6.23] oppure, per una trattazione più generale all'interno della teoria delle superfici di Riemann, [2, Th. 14.12].

Da questo teorema è assai semplice ricavare il teorema di esistenza di Riemann.

Teorema 1.25 (Esistenza di Riemann)**.** *Sia $\mathcal{X}$ una superficie di Riemann compatta, $\{\mathcal{P}_1, \dots, \mathcal{P}_n\}$ un insieme di punti distinti e $\{c_1, \dots, c_n\}$ un insieme di valori in $\mathbb{C}$. Esiste una funzione meromorfa $f : \mathcal{X} \to \mathbb{C}$ tale che:*

$$f(\mathcal{P}_i) = c_i \ \forall 1 \leq i \leq n.$$

Dimostrazione. Siano $f_i : \mathcal{X} \to \mathbb{C}$ ognuna con polo solamente in $\mathcal{P}_i$ come da teorema 1.24. Possiamo allora definire le seguenti funzioni:

$$g_{ij} := \frac{f_i - f_i(\mathcal{P}_j)}{f_i - f_i(\mathcal{P}_j) + d_{ij}}$$

per $i \neq j$, con d_{ij} costanti non nulle tali che il denominatore non si annulli su nessun punto tra i $\mathcal{P}_k$. Allora $g_{ij}(\mathcal{P}_i) = 1$, $g_{ij}(\mathcal{P}_j) = 0$ e $g_{ij}(\mathcal{P}_k) \neq \infty$ per ogni $k \neq i, j$. Pertanto per il prodotto $h_i := \prod_{j \neq i} g_{ij}$ vale $h_i(\mathcal{P}_j) = \delta_{ij}$. Basta allora porre

$$f := \sum_{i=1}^{n} c_i h_i$$

per ottenere la funzione richiesta. □

Grazie a questo risultato possiamo stabilire una corrispondenza biunivoca tra estensioni di campo di $\mathbb{C}(t)$ e rivestimenti ramificati di $\mathbb{P}^1(\mathbb{C})$. Con questa corrispondenza potremo studiare la struttura dei gruppi di Galois su $\mathbb{C}(t)$ con mezzi topologici; studiamo allora le proprietà dei rivestimenti ramificati.

Stabiliamo prima la notazione.

Definizione 1.26. Sia $\mathcal{X}$ una superficie di Riemann e $\pi : \mathcal{Y} \to \mathcal{X}$ un suo rivestimento ramificato. Chiameremo:

- $\mathcal{M}(\mathcal{X})$ il campo delle funzioni meromorfe su $\mathcal{X}$.

- π^* la mappa $\mathcal{M}(\mathcal{X}) \to \mathfrak{M}(\mathcal{Y})$ che manda $f \to f \circ \pi$.
- Deck(π) il gruppo di automorfismi del rivestimento π, ovvero gli automorfismi $g : \mathcal{Y} \to \mathcal{Y}$ per i quali $\pi = \pi \circ g$.
- D il disco unitario $\{z \in \mathbb{C} \mid |z| < 1\}$.
- D^* il disco unitario privato dell'origine $D \setminus \{0\}$.

Lemma 1.27. *Un rivestimento non ramificato $\pi : \mathcal{Y} \to \mathcal{X}$ di una superficie di Riemann induce su $\mathcal{Y}$ una struttura di superficie di Riemann; con tale struttura gli omomorfismi di rivestimenti diventano olomorfismi.*

Tale struttura è l'unica che rende π un olomorfismo.

Dimostrazione. Sia (U_α, z_α) un atlante di $\mathcal{X}$ tale per cui $\pi^{-1}(U_\alpha)$ è unione disgiunta di aperti V_α omeomorfi a U_α. Ci basta verificare che $(V_\alpha, z_\alpha \circ \pi)$ è un atlante di $\mathcal{Y}$. Le mappe $z_\alpha \circ \pi$ sono evidentemente omeomorfismi da V_α nel disco unitario $\pi(U_\alpha) = D$; dati V_α e $V_{\alpha'}$ a intersezione non vuota, $(z_{\alpha'} \circ \pi) \circ (z_\alpha \circ \pi)^{-1} = z_{\alpha'} \circ \pi \circ \pi^{-1} \circ z_\alpha^{-1} = z_{\alpha'} \circ z_\alpha^{-1}$ è una mappa analitica (considerando le opportune restrizioni). Tale atlante definisce univocamente la struttura di superficie di Riemann su $\mathcal{Y}$, pertanto è l'unica che rende π un olomorfismo.

Siano ora π e π' due rivestimenti da due superifici $\mathcal{Y}$ e $\mathcal{Z}$ su $\mathcal{X}$, tali per cui esista una funzione continua $\phi : \mathcal{Y} \to \mathcal{Z}$ per il quale $\pi = \pi' \circ \phi$. Allora localmente vale $\phi = \pi'^{-1} \circ \pi$ (scelta un opportuna inversa locale di π'), quindi ϕ è un biolomorfismo locale, quindi è un olomorfismo. □

Quest'ultima affermazione vale anche per i rivestimenti ramificati a patto di classificarne il comportamento locale.

Proposizione 1.28. *Sia $\pi : \mathcal{X} \to D^*$ un rivestimento di grado n del disco unitario senza centro $D^* := \{z \in \mathbb{C} \mid 0 < |z| < 1\}$. Allora esiste un omeomorfismo $\phi : \mathcal{X} \to D^*$ tale che $\pi = (\phi)^n$.*

Dimostrazione. Il rivestimento dato dalla mappa $\exp : \mathbb{H} \to D^*$, dove $\mathbb{H} = \{z \in \mathbb{C} \mid \Re(z) < 0\}$, è un rivestimento universale poiché $\mathbb{H}$ è semplicemente connesso; esiste pertanto una mappa continua $\psi : \mathbb{H} \to \mathcal{X}$ tale che $\pi \circ \psi = \exp$. Il sottogruppo di Deck$(\exp) \cong \mathbb{Z}$ associato a ψ è quindi $n\mathbb{Z}$; il suo generatore agisce su $\mathbb{H}$ come traslazione $z \mapsto z + 2\pi\imath n$. Ora la mappa $g(z) := \exp(z/n)$ è un rivestimento di D^* che ha come sottogruppo associato lo stesso $n\mathbb{Z}$, quindi è omeomorfo tramite una ϕ a $\mathcal{X}$ in modo che $g = \phi \circ \psi$. Evidentemente abbiamo $(g)^n = \exp$.

Basta ora verificare $(\phi \circ \psi)^n = (g)^n = \exp = \pi \circ \psi$. Essendo ψ surgettiva abbiamo la relazione desiderata. □

Proposizione 1.29. *Sia $\mathcal{X}$ una superficie di Riemann e $\mathcal{S}$ un suo sottoinsieme discreto di punti; poniamo $\mathcal{X}' := \mathcal{X} \setminus \mathcal{S}$. Se $\pi' : \mathcal{Y}' \to \mathcal{X}'$ è un rivestimento proprio non ramificato esiste una superficie $\mathcal{Y}$, un rivestimento ramificato $\pi : \mathcal{Y} \to \mathcal{Y}$ e un biolomorfismo $\phi : \mathcal{Y}' \to \mathcal{Y} \setminus \pi^{-1}(\mathcal{S})$ tale per cui $\pi \circ \phi = \pi'$. Inoltre* Deck$(\pi) \cong$ Deck(π').

Dimostrazione. Sia $\mathcal{P} \in \mathcal{S}$ e prendiamo una carta centrata in $\mathcal{P}$, ovvero un aperto $U_\mathcal{P} \ni \mathcal{P}$ e una mappa $z_\mathcal{P} : U_\mathcal{P} \to D$ per la quale $z_\mathcal{P}(\mathcal{P}) = 0$, tale per cui π' è un omeomorfismo con le componenti connesse della sua controimmagine. In questo modo $z_\mathcal{P} \circ \pi'$ diventa un rivestimento da ogni sua componente connessa nel disco senza centro D^*; essendo la mappa propria, il suo grado è finito ed esiste un omeomorfismo $\phi : {\pi'}^{-1}(U_\mathcal{P}) \to D^*$ per il quale $\pi' = (\phi)^n$. Per il lemma 1.27 tale omeomorfismo è un biolomorfismo.

Di nuovo, per proprietà della mappa π', esistono solo un numero finito di componenti connesse $V^i_\mathcal{P}$ in ${\pi'}^{-1}(U_\mathcal{P})$; associamo ad ognuna di esse un nuovo punto $\mathcal{P}^i$ ed estendiamo la topologia con gli aperti della forma ${\pi'}^{-1}(A) \cup \{\mathcal{P}^i\}$ al variare di A aperto contenente $\mathcal{P}$ in $\mathcal{X}$. La topologia indotta resta di Hausdorff, ed estendendo le mappe ϕ ponendo $\phi(\mathcal{P}^i) = 0$ si verifica facilmente che la struttura di superficie di Riemann indotta da π' su $\mathcal{Y}'$ si estende su $\mathcal{Y} := \mathcal{Y} \cup \{\mathcal{P}^i\}$. Poniamo infine $\pi|_{\mathcal{Y}'} = \pi'$ e $\pi(\mathcal{P}^i) = \mathcal{P}$ e otteniamo il rivestimento richiesto.

$\mathrm{Deck}(\pi)$ si mappa su $\mathrm{Deck}(\pi')$ tramite restrizione. Se supponiamo che un automorfismo lasci fisso $\mathcal{Y}'$, anche i punti $\mathcal{P}^i$ resteranno fissi; per verificarlo basta prendere un suo intorno aperto connesso V omeomorfo alla sua immagine tramite π e notare che l'automorfismo può solo lasciare $V \setminus \{\mathcal{P}^i\}$ fisso o mandarlo in un altro aperto da lui disgiunto. Di conseguenza $\mathcal{P}$ non può essere mandato in un'altra componente connessa e resta fisso.

La mappa è anche surgettiva, poiché si estende naturalmente considerando l'azione appena indicata di $\mathrm{Deck}(\pi')$ sui suoi intorni aperti. □

Il teorema appena visto ha un interessante inverso:

Proposizione 1.30. *Sia $f : \mathcal{Y} \to \mathcal{X}$ una mappa olomorfa non costante fra superficie di Riemann. Esistono due atlanti di $\mathcal{X}$ e $\mathcal{Y}$ tali per cui la mappa f, localmente, è rappresentata da $z \mapsto z^k$ con $k \in \mathbb{Z}$.*

Dimostrazione. Sia (U, z) un atlante di $\mathcal{X}$ e (V, s) un atlante di $\mathcal{Y}$. A meno di raffinare l'atlante di $\mathcal{Y}$, supponiamo che per ogni V si abbia $f(V) \subset U$ per qualche U. Supponiamo inoltre, a meno di aumentare il numero di carte, che ogni punto $\alpha \in \mathcal{Y}$ abbia una carta nel quale $s(\alpha) = 0$; lo stesso si supponga per $\mathcal{X}$.

La mappa $\phi := z \circ f \circ s^{-1}$ è una mappa analitica del disco D in sé non costante con $\phi(0) = 0$. Possiamo allora scrivere $\phi(y) = y^k g(y)$, con $g(0) \neq 0$. Esiste quindi un disco D' sufficientemente piccolo nel quale si possa scrivere $g(y) = h(y)^k$, con h olomorfa. La mappa $\psi := yh(y)$ è localmente inveribile nell'origine; sia $s' := \psi \circ s$. Vale quindi:

$$z \circ f \circ {s'}^{-1} = z \circ f \circ s^{-1} \circ \psi^{-1} = \phi \circ \psi^{-1} = (\psi^{-1} \circ \psi)^k = z^k.$$

Restringendo opportunamente i domini U e V e riscalando le due mappe in modo che vadano sull'intero disco unitario otteniamo due carte nelle quali f è rappresentata da $z \mapsto z^k$. □

Definizione 1.31. Chiamiamo *indice di ramificazione di f in $\mathcal{P} \in \mathcal{Y}$* l'esponente k della proposizione 1.30.

Proposizione 1.32. *Sia $f : \mathcal{Y} \to \mathcal{X}$ una funzione olomorfa non costante tra superfici di Riemann compatte. Allora f è un rivestimento ramificato.*

Dimostrazione. Localmente l'azione di f è della forma $z \mapsto z^k$. Dalla dimostrazione della proposizione 1.30 deduciamo che i punti per i quali si ha $k > 1$ sono gli zeri della derivata di f vista localmente; pertanto accadrà solo su un insieme finito discreto A di punti. Per tutti i punti di $\mathcal{Y}' := \mathcal{Y} \setminus A$ abbiamo quindi che f è aperta e localmente invertibile, quindi un omeomorfismo locale. È anche una mappa propria, in quanto fra compatti, quindi è un rivestimento.

Riaggiungendo i punti A otteniamo un rivestimento ramificato. □

Definizione 1.33. Sia $\pi : \mathcal{Y} \to \mathcal{X}$ un rivestimento ramificato finito di superfici di Riemann. Per ogni aperto U sufficientemente piccolo in $\mathcal{X}$ prendiamo le componenti V_i e le mappe τ_i inverse locali di π. Data una funzione $f \in \mathcal{M}(\mathcal{Y})$ definiamo $f_i := f \circ \tau_i$ e scriviamo il polinomio:

$$p(x) = \prod_{i=1}^{n}(x - f_i) = x^n + c_1 x^{n-1} + \ldots + c_n. \tag{1.3.1}$$

I coefficienti c_i sono detti *funzioni simmetriche di f rispetto a π*.

Osservazione 1.34. Le funzioni simmetriche sono ben definite su tutto $\mathcal{X}$ e sono meromorfe.

Teorema 1.35. *Sia $\pi : \mathcal{Y} \to \mathcal{X}$ un rivestimento ramificato finito di superfici di Riemann compatte. Allora il campo $\mathcal{M}(\mathcal{Y})$ su $\mathcal{Y}$ è algebrico su $\mathcal{M}(\mathcal{X})$ attraverso l'immersione π^* e vale la relazione:*

$$\mathrm{Deck}(\pi) \cong \mathrm{Aut}(\mathcal{M}(\mathcal{Y})/\mathcal{M}(\mathcal{X}))$$

Il grado dell'estensione di campi è uguale al grado del rivestimento, e l'uno è normale solo quando l'altro è normale.

Dimostrazione. Sia $p(x)$ un polinomio come nell'equazione (1.3.1). Dato che localmente vale $\pi^* f_i = f$ si deduce che che f è localmente radice del polinomio $p^*(x)$ con coefficienti $c_i^* := \pi^*(c_i)$, quindi è algebrico di grado al più n su $\pi^*(\mathcal{M}(\mathcal{X}))$.

Per estendere il teorema al caso ramificato basta applicarlo al rivestimento $\pi' : \mathcal{Y}' \to \mathcal{X}'$ ricavato dal precedente eliminando i soli punti di ramificazione; basta poi notare che una funzione $f \in \mathcal{M}(\mathcal{Y}')$ si estende su $\mathcal{Y}$ solo quando i coefficienti c_i del suo polinomio si estendono su $\mathcal{X}$. Infatti se f si estende, i coefficienti si estendono banalmente anch'essi; mentre quando i coefficienti si estendono su un punto $\mathcal{P}$ localmente su $\mathcal{Y}$ f verifica un polinomio a coefficienti limitati, pertanto è limitata anch'essa e si può estendere.

Il grado dell'estensione di campi è quindi al più n; prendiamo ora con il teorema di esistenza di Riemann una funzione f_0 che sulla fibra di un punto non ramificato assuma valori tutti distinti. Se soddisfacesse un polinomio di grado $m < n$ non potrebbe assumere più di m valori possibili, poiché ciascuna delle f_i soddisferebbe un polinomio fissato di grado m. Pertanto l'estensione è di grado n.

Ora $\alpha \in \mathrm{Deck}(\mathcal{Y}/\mathcal{X})$ agisce evidentemente come automorfismo di campi mappando $f \mapsto f \circ \alpha$. Il suo campo fisso contiene evidentemente $\mathcal{M}(\mathcal{X})$. L'azione di un automorfismo non banale però permuta sempre almeno due punti della fibra di un punto non ramificato, per cui l'azione su f_0 non è banale e $\mathrm{Deck}(\mathcal{M}(\mathcal{Y})/\mathcal{M}(\mathcal{X}))$ si immerge iniettivamene in $\mathrm{Aut}(\mathcal{M}(\mathcal{Y})/\mathcal{M}(\mathcal{X}))$.

Verifichiamo ora che l'immersione è anche surgettiva. Il polinomio minimo di f_0 è separabile, pertanto il suo discriminante sarà una funzione su $\mathcal{Y}$ meromorfa non nulla; i punti dove esso si annulla saranno quindi un insieme discreto. Considerando quindi la superficie $\mathcal{Y}'$ ottenuta eliminando tali punti (che saranno un'unione finita di fibre) abbiamo che f_0 assume solo valori distinti sulle fibre e definisce pertanto una permutazione di tali punti ogni qualvolta che si applichi un automorfismo del campo. L'azione su f_0 è però della forma $f_0 \mapsto a_0 + a_1 f_0 + \cdots + a_{n-1} f_0^{n-1}$, per cui prendendo un aperto sufficientemente piccolo in $\pi(\mathcal{Y}')$ l'azione sulle controimmagini permuterà le componenti connesse. Pertanto, essendo localmente un biolomorfismo ed essendo una mappa bigettiva l'automorfismo di campo è implementato da un automorfismo di rivestimento. L'automorfismo si estende ora in modo unico per la proposizione 1.29.

L'affermazione sulla normalità è ora conseguenza del fatto che se f_0 ha n coniugati distinti, allora il suo valore in un punto della fibra deve variare su tutti gli n possibili, quindi gli automorfismi di rivestimento associati agiscono transitivamente sulla fibra. Viceversa, se l'azione di $\mathrm{Deck}(\pi)$ sulle fibre è transitiva allora f_0 ha n coniugati distinti. □

Vale anche il risultato inverso:

Teorema 1.36. *Sia $\mathcal{X}$ una superficie di Riemann compatta e L una estensione algebrica finita di $\mathcal{M}(\mathcal{X})$. Allora esiste una superficie $\mathcal{Y}$ ed un rivestimento ramificato $\pi : \mathcal{Y} \to \mathcal{X}$ per cui si abbia*

$$L/\mathcal{M}(\mathcal{X}) \cong \mathcal{M}(\mathcal{Y})/\mathcal{M}(\mathcal{X}).$$

Dimostrazione. Innanzitutto prendiamo $p(x)$ il polinomio minimo di un generatore f_0 dell'estensione. Essendo irriducibile, il suo discriminante è una funzione meromorfa non nulla su $\mathcal{X}$, quindi si annulla solo su un insieme discreto A. Chiamiamo $\mathcal{X}' := \mathcal{X} \setminus A$.

Prendiamo una carta (U, z) con $z : D \to U$ omeomorfismo centrata in un punto $\mathcal{P} \in \mathcal{X}'$. Possiamo vedere localmente il polinomio $p(x)$ come funzione a due variabili $\tilde{p}(w, x)$:

$$\tilde{p}(w, x) = x^n + (c_1 \circ z^{-1})(w) x^{n-1} + \ldots (c_n \circ z^{-1})$$

con $w \in D$; abbiamo la condizione che $\tilde{p}(0, x)$ ha radici distinte. Allora, per la proposizione 1.16, esistono n funzione ϕ_i' tale che $\tilde{p}(w, \phi_i'(w)) = 0$ identicamente in un intorno di 0. Siano $\phi_i = \phi_i' \circ z^{-1}$.

Sia ora $\mathcal{Y}'$ lo spazio delle coppie $(\mathcal{P}, A, \phi)$, dove A è un intorno di $\mathcal{P}$ in $\mathcal{X}'$ e ϕ una funzione olomorfa su A tale che $p(\phi) = 0$. Abbiamo appena visto che se A è sufficientemente piccolo esistono n di tali funzioni distinte. Quozientiamo ora lo spazio per la relazione $\sim$, dove $(\mathcal{P}, A, \phi) \sim (\mathcal{P}', A', \phi')$

se $\mathcal{P} = \mathcal{P}'$ e $\phi|_{A\cap A'} = \phi'|_{A\cap A'}$. Usiamo come base di aperti gli insiemi della forma $B_{U,f} := \{(\mathcal{P}, A, \phi)^\sim \mid \mathcal{P} \in U \wedge U \subset A \wedge \phi|_U = f\}$ al variare di U aperto in $\mathcal{X}'$ e f funzione olomorfa su U. Tale spazio è evidentemente di Hausdorff.

Definiamo ora $\pi' : \mathcal{Y}' \to \mathcal{X}'$ come la mappa che manda $(\mathcal{P}, A, \phi)^\sim$ in $\mathcal{P}$. Per quanto visto ogni punto di $\mathcal{X}'$ ha un intorno U sul quale esistono funzioni $\phi_1, \ldots, \phi_n$ distinte che annullino $p(x)$, con la proprietà aggiuntiva che i loro valori siano distinti su tutto U; pertanto $\pi'^{-1}(U)$ sarà l'unione disgiunta degli B_{U,ϕ_i}. Inoltre π' è evidentemente un omeomorfismo con l'immagine su tali aperti, quindi è un rivestimento.

Di conseguenza, per la proposizione 1.27, $\mathcal{Y}'$ è una superficie di Riemann (a meno di verificarne la connessione). π' ha grado finito n, pertanto è una mappa propria e per la proposizione 1.29 si può estendere a $\pi : \mathcal{Y} \to \mathcal{X}$, con $\mathcal{Y}$ compatta.

Su $\mathcal{Y}'$ è definita una funzione f_0 che soddisfa il polinomio $p(x)$: basta prendere $f_0((\mathcal{P}, A, \phi)^\sim) := \phi(\mathcal{P})$. Tale funzione si estende naturalmente su $\mathcal{Y}$, poiché i coefficienti del polinomio sono definiti in realtà su tutto $\mathcal{X}$.

Per vedere la connessione di $\mathcal{Y}$ basta notare che se vi fossero più componenti connesse, ognuna di queste fornirebbe un rivestimento di $\mathcal{X}$ di grado minore di n; pertanto f_0 avrebbe polinomio minimo di grado minore di n e il polinomio $p(x)$ sarebbe riducibile, contro l'ipotesi. □

Teorema 1.37. *L'associazione appena stabilita è biunivoca, nel senso che due rivestimenti π, π' di grado finito di una superficie $\mathcal{X}$ sono omeomorfi se e soltanto se le estensioni di campo delle funzioni meromorfe sono isomorfe.*

Dimostrazione. Se due rivestimenti π e π', da $\mathcal{Y}$ e $\mathcal{Y}'$, sono omeomorfi tramite ϕ, la mappa $f \mapsto f \circ \phi$ è chiaramente un isomorfismo di campi ϕ^* per il quale $\pi' \circ \phi^* = \pi$.

Per il passo inverso è sufficiente verificare che un rivestimento di grado finito è omeomorfo alla superficie costruita nel teorema 1.36. Sia $\pi : \mathcal{Y} \to \mathcal{X}$ un rivestimento di grado finito, f_0 un generatore dell'estensione di campi e $p(x)$ il suo polinomio minimo. Siano $\mathcal{X}'$ e $\mathcal{Y}'$ le superfici private dei punti che annullano il discriminante di $p(x)$ e delle loro controimmagini per π, che saranno un insieme discreto e quindi finito; f_0 assumerà valori distinti sulle fibre. Definiamo la mappa $\phi : (\mathcal{P}, A, \phi)^\sim \mapsto \mathcal{P}^i$, dove $\mathcal{P}^i$ è il punto di $\mathcal{Y}'$ tale per cui $f_0(\mathcal{P}^i) = \phi(\mathcal{P})$. È chiaramente un omeomorfismo. Per la proposizione 1.29 esiste un solo modo per reintrodurre i punti che annullano il discriminante di $p(x)$ compatibilmente con le mappe di rivestimento, quindi l'omeomorfismo si estende a tutta la superficie $\mathcal{Y}$. □

Con questo bagaglio di strumenti concludiamo quindi che i rivestimenti di grado finito di $\mathbb{P}^1(\mathbb{C})$, la retta complessa, sono in corrispondenza biunivoca con le estensioni finite del suo campo di funzioni $\mathbb{C}(t)$ (a meno di isomorfismo); rivestimenti normali vanno in estensioni normali. Inoltre, per il teorema di esistenza di Riemann, su ogni superficie compatta esiste una funzione meromorfa non costante; essa sarà quindi, per la proposizione 1.32, un rivestimento di $\mathbb{P}^1(\mathbb{C})$, quindi tutte le superfici compatte sono identificate a meno di biolomorfismo con le estensioni finite di $\mathbb{C}(t)$.

Per concludere l'identificazione stabiliamo anche la corrispondenza tra punti $\mathcal{P} \in \mathcal{X}$ e in posti $\mathfrak{P} \in \mathbb{P}(\mathcal{M}(\mathcal{X})/\mathbb{C})$.

Teorema 1.38. *Sia $\pi : \mathcal{X} \to \mathbb{P}^1(\mathbb{C})$ un rivestimento ramificato di grado finito.*

Allora per ogni punto $\mathcal{P} \in \mathcal{X}$ l'insieme delle funzioni che si annullano su $\mathcal{P}$ è un posto $\mathfrak{P} \in \mathbb{P}(\mathcal{M}(\mathcal{X})/\mathbb{C})$; viceversa, il luogo di zeri di un posto $\mathfrak{P}$ è un punto $\mathcal{P}$.

Inoltre ogni posto ha indice di ramificazione su $\mathbb{P}(\mathbb{C}(t)/\mathbb{C})$ rispetto all'immersione π^* uguale all'indice di ramificazione del punto associato rispetto a π.

Dimostrazione. L'anello delle funzioni olomorfe in $\mathcal{P}$ è evidentemente un anello di valutazione discreta $(\mathcal{O}, \mathfrak{P})$, con $\mathfrak{P}$ ideale delle funzioni che si annullano in $\mathcal{P}$. Ovviamente $\mathbb{C}^* \subset \mathcal{O}^*$, pertanto $\mathfrak{P}$ è un posto di $\mathbb{P}(\mathcal{M}(\mathcal{X})/\mathbb{C})$.

Prendiamo ora $\mathfrak{P}$ e sia $\mathfrak{P}' := \mathfrak{P} \cap \mathbb{C}(t)$. Quest'ultimo è un posto non banale di $\mathbb{C}(t)/\mathbb{C}$, pertanto si annulla su un punto $\mathcal{P} \in \mathbb{P}^1(\mathbb{C})$. Un elemento f di $\mathfrak{P}$ avrà polinomio minimo con termine noto in $\mathfrak{P}$, quindi nullo in $\mathcal{P}$, pertanto si dovrà annullare su almeno un punto della fibra di $\mathcal{P}$. Supponiamo che vi sia un altro elemento $g \in \mathfrak{P}$ che non si annulli in nessun punto della fibra di $\mathcal{P}$ dove già si annulla f; esiste allora una loro combinazione lineare $\alpha f + \beta g$ a coefficienti in $\mathbb{C}^*$ che non si annulli in nessun punto della fibra. Tale elemento appartiene però a $\mathfrak{P}$, quindi per la stessa ragione di f e g deve annullarsi su un punto della fibra. Quindi f e g hanno uno zero comune. Per concludere, supponiamo che il luogo degli zeri di $\mathfrak{P}$ contenga due punti distinti $\mathcal{P}_1$ e $\mathcal{P}_2$. Per il teorema di esistenza di Riemann esiste una funzione h nulla su $\mathcal{P}_1$ e non nulla su $\mathcal{P}_2$; allora $h \notin \mathfrak{P}$, quindi $h^{-1} \in \mathcal{O}_{\mathfrak{P}}$. Per un esponente abbastanza grande $h^{-k}f$ non ha zero in $\mathcal{P}_1$, ma deve appartenere a $\mathfrak{P}$, quindi $\mathcal{P}_1$ non appartiene al suo luogo di zeri. Assurdo.

Per controllare gli indici di ramificazione ci basta considerare che localmente π in un punto di ramificazione $\mathcal{P}$ agisce come $z \mapsto z^e$, quindi se una $f \in \mathbb{P}^1(\mathbb{C})$ annulla con ordine in $\pi(\mathcal{P})$ allora $\pi^*(f)$ si annulla con ordine e in $\mathcal{P}$. Gli indici di ramificazione pertanto coincidono. □

Studiamo quindi i rivestimenti di grado finito di $\mathbb{P}^1(\mathbb{C})$, con la condizione aggiuntiva che il luogo di ramificazione sia interamente contenuto in un insieme finito $\mathcal{S}$ di cardinalità $s \in \mathbb{N}$, sapendo che vi corrisponderanno le estensioni di $\mathbb{C}(t)$ ramificate solo su un insieme fissato S di posti. Il primo passo, ovviamente, è calcolare il rivestimento universale della retta complessa.

Teorema 1.39 (Hurwitz)**.** *Sia $\mathcal{S} = \{\mathcal{P}_1, \dots, \mathcal{P}_s\}$ un insieme di punti di $\mathbb{P}^1(\mathbb{C})$ e $\mathcal{P}_0$ un punto base fuori da $\mathcal{S}$. Allora si ha che:*

$$\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S; \mathcal{P}_0) \cong \langle \gamma_1, \dots, \gamma_s | \gamma_1 \cdots \gamma_s = e \rangle.$$

Dimostrazione. Se $s = 1$ la nostra superficie è omeomorfa a $\mathbb{C}$, che è contrattile, pertanto con π_1 banale. Se $s = 0$ allora la retta complessa è unione di $\mathbb{C}$ e $\mathbb{P}^1(\mathbb{C}) \setminus \{0\}$; sono entrambi semplicemente connessi perché contrattili e la loro intersezione è connessa, quindi per il teorema di Van Kampen è semplicemente connessa.

Trascuriamo d'ora in poi la scelta del punto base; i gruppi fondamentali sono comunque isomorfi. Se $s > 1$, a meno di inversione possiamo supporre

che $\infty \in \mathcal{S}$. Calcoliamo prima $\pi_1(\mathbb{C} \setminus \mathcal{S})$. Con un opportuno omeomorfismo spostiamo i punti di $\mathcal{S} \cap \mathbb{C}$ sui punti $\{1, \dots, s-1\}$ (ad esempio scegliendo una retta tale per cui le proiezioni dei punti di $\mathcal{S}$ su di essa siano tutte distinte, poi deformando il piano lungo la retta perpendicolare e infine deformando lungo la retta stessa per equidistanziare i punti; per finire una rototraslazione). Dividiamo il piano in fasce $F_1 := \{z \mid \Re(z) < 1\}$, $F_i := \{z \mid i-1 < \Re(z) < i+1\}$ per $1 < i < s-1$, $F_{s-1} := \{z \mid \Re(z) > s-2\}$. La loro unione è $\mathbb{C}$, mentre le loro intersezioni due a due sono semplicemente connesse. Il π_1 di ognuna di esse è il gruppo fondamentale del piano senza l'origine, pertanto ciclico infinito; per il teorema di Van Kampen applicato induttivamente a $F_1 \cup F_2$, $F_1 \cup F_2 \cup F_3$, ... otteniamo che il gruppo fondamentale del piano senza $s-1$ punti è il gruppo libero generato da $s-1$ elementi che chiameremo $\gamma_1, \dots, \gamma_{s-1}$. Prediamo ora un disco D centrato nell'origine di raggio $s+1$ e il complementare C di un disco chiuso centrato nell'origine di raggio s. Il gruppo fondamentale di D è il gruppo appena descritto; il gruppo fondamentale di C è ciclico infinito (invertendo $z \mapsto 1/z$ C diventa un disco privato del centro). Il π_1 di $C \cap D$ è di nuovo $\mathbb{Z}$, e il suo generatore identifica il cammino $\gamma_1 \cdots \gamma_{s-1}$ con un generatore γ_s^{-1} di $\pi_1(C)$. Pertanto, per Van Kampen, il gruppo risultante per qualsiasi scelta del punto base sarà isomorfo al gruppo di s generatori con la relazione $\gamma_1 \cdots \gamma_s = e$. □

Il rivestimento universale di $\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$ ha pertanto gruppo di automorfismi isomorfo al gruppo indicato. Esso è però infinito, per cui la corrispondenza con le estensioni di campi non si estende come nel teorema 1.35. Dobbiamo quindi fare un passo aggiuntivo.

Teorema 1.40 (RET profinito)**.** *Sia S un insieme finito di posti di $\mathbb{C}(t)$ e $\mathcal{S}$ il corrispondente insieme di punti di $\mathbb{P}^1(\mathbb{C})$. Chiamiamo N_S l'estensione massima di $\mathbb{C}(t)$ in una chiusura algebrica $\overline{\mathbb{C}(t)}$ che sia ramificata solo in S; allora vale per ogni $\mathcal{P}_0$:*

$$\mathrm{Gal}(N_S/\mathbb{C}(t)) \cong \hat{\pi}_1(\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}; \mathcal{P}_0)$$

Dimostrazione. Chiamiamo π il rivestimento universale di $\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$. Ad ogni sottogruppo normale di indice finito N è associato un rivestimento $\tilde{\pi} : \mathcal{Y} \to \mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$ con gruppo di automorfismi isomorfo al quoziente per N. Compattifichiamo con la proposizione 1.29 e applichiamo il teorema 1.35: ad ogni sottogruppo normale N di indice finito in $\mathrm{Deck}(\pi)$ corrisponde un'estensione di Galois $M_N/\mathbb{C}(t)$ con gruppo isomorfo al quoziente, ramificata solamente in S. Viceversa per ogni estensione normale finita M esiste un rivestimento ramificato in $\mathcal{S}$ al quale corrisponde un sottogruppo normale di indice finito N_M. Ci basta quindi esplicitare il completamento profinito:

$$\begin{aligned}
\hat{\pi}_1(\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}; P_0) &\cong \varprojlim_N \frac{\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}; P_0)}{N} \\
&\cong \varprojlim_M \mathrm{Gal}(M/\mathbb{C}(t)) \\
&\cong \mathrm{Gal}(N_S/\mathbb{C}(t)).
\end{aligned}$$

□

Chiamiamo d'ora in poi Γ_s il gruppo $\mathrm{Gal}(N_S/\mathbb{C}(t))$. Possiamo raffinare il teorema appena enunciato analizzando l'azione dei generatori γ_i sugli elementi del campo:

Teorema 1.41. *Sia $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ un insieme di posti di $\mathbb{C}(t)$ e siano γ_i i rispettivi generatori di Γ_s costruiti secondo le indicazioni dei teoremi precedenti. Esistono allora delle estensioni $\overline{\mathfrak{P}}_i$ dei posti in N_S tali per cui:*

$$\forall 1 \leq i \leq n \quad \overline{\langle \gamma_i \rangle} = I(\overline{\mathfrak{P}}_i/\mathfrak{P}_i).$$

Dimostrazione. Sia $\pi : \mathcal{U} \to \mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$ un rivestimento universale secondo la notazione del teorema precedente, $\mathcal{P}_0$ un punto base in $\mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$ e $\overline{\mathcal{P}}_0$ un suo sollevamento fissato in $\mathcal{U}$; prendiamo poi rivestimento finito $\tilde{\pi} : \mathcal{Y} \to \mathbb{P}^1(\mathbb{C})$ con la proiezione $\delta : \mathcal{U} \to \mathcal{Y}$.

Un cammino c_i rappresentante la classe di omotopia γ_i si solleva in modo unico ad un cammino $\tilde{c}_i$ tale per cui $\tilde{c}_i(0) = v(\overline{\mathcal{P}}_0) = \tilde{\mathcal{P}}_0$. Possiamo, tramite omotopia, trasformare il cammino c_i in un cammino doppio da $\mathcal{P}_0$ a $\mathcal{P}_i$ (rientrando nella compattificazione $\mathbb{P}^1(\mathbb{C})$), e il suo nuovo sollevamento $\tilde{c}_i$ identificherà un punto $\tilde{\mathcal{P}}_i$ della fibra $\pi^{-1}(\mathcal{P}_i)$. In questo modo possiamo associare ad ognuno dei cammini un'azione d_i sul rivestimento definita da $d_i(\tilde{\mathcal{P}}_0) = \tilde{c}_i(1)$ con la proprietà che $d_i(\tilde{\mathcal{P}}_i) = \mathcal{P}_i$.

Sia ora $\tilde{\mathfrak{P}}_i$ il posto associato a $\tilde{\mathcal{P}}_i$. L'azione dei d_i sul campo di funzioni, che chiameremo σ_i, lascia evidentemente invariato $\tilde{\mathfrak{P}}_i$, pertanto appartiene al suo gruppo di decomposizione; avendo $\mathfrak{P}_i$ campo residuo $\mathbb{C}$, esso è proprio il gruppo di inerzia. Se invece prendiamo un automorfismo di campo che lasci fisso $\tilde{\mathfrak{P}}_i$, la trasformazione associata sul rivestimento lascia fisso $\tilde{\mathcal{P}}_i$; dovrà allora essere una potenza di d_i.

Abbiamo quindi ottenuto che σ_i genera il gruppo d'inerzia $I(\tilde{\mathfrak{P}}_i/\mathfrak{P}_i)$, mentre il limite proiettivo dei σ_i nel gruppo Γ_s è proprio γ_i; prendendo quindi $\overline{\mathfrak{P}}_i = \bigcup_{M \subset N_S} \tilde{\mathfrak{P}}_i$ deduciamo la tesi. □

1.4 Discesa a $\overline{k}$

Il passo successivo che ci serve per poter proseguire la nostra ricerca di gruppi su $\mathbb{Q}$ è trasferire i teoremi appena enunciati su campi algebricamente chiusi più piccoli; il nostro obiettivo sarà in effetti parlare di $\overline{\mathbb{Q}}$. In generale al teorema di Riemann si applica principio di Lefschetz, quindi i risultati della sezione precedente hanno validità su *tutti* i campi algebricamente chiusi di caratteristica zero. Ci accontenteremo però di una breve dimostrazione ristretta ai soli sottocampi di $\mathbb{C}$.

Diamo prima una definizione che ci sarà utile anche in seguito:

Definizione 1.42. Siano N/K un'estensione di campi e G un gruppo di suoi automorfismi. Un sottocampo $K' \subset K$ si dice *campo di definizione di N/K,*

oppure che N/K *è definito su* K', se esiste una sottoestensione $N_{K'}$ tale che:

$$N_{K'} \cap K = K', \quad N_{K'}K = N.$$

Se inoltre $N_{K'}$ è invariante per l'azione di G, K' si dice *campo di definizione di* N/K *con* G, o che $N/_G K$ *è definito su* K'.

Stabiliamo inoltre un lemma anch'esso utile:

Lemma 1.43. *Sia $\overline{k}$ un campo algebricamente chiuso e $\mathfrak{P}$ un posto in $\mathbb{P}(\overline{k}(t)/\overline{k})$. Se z è un generatore di $\mathfrak{P}$, allora il completamento $\overline{k}_{\mathfrak{P}}$ è isomorfo a $\overline{k}((z))$ identificando $\overline{k}$ e z.*

Se $N/k(t)$ è un'estensione finita e $\tilde{\mathfrak{P}}$ è un'estensione di $\mathfrak{P}$ in N, allora $N_{\tilde{\mathfrak{P}}}$ è isomorfo a $\overline{k}((s))$ con $s^e = z$, per z generatore di $\mathfrak{P}$ e $e := e(\tilde{\mathfrak{P}}|\mathfrak{P})$.

Se inoltre $N/\overline{k}(t)$ è normale, l'azione il gruppo di inerzia è ciclico e l'azione di un generatore sul completamento $\overline{k}((s))$ è di fissare $\overline{k}$ e moltiplicare s per una radice primitiva e-esima dell'unità.

Dimostrazione. z è della forma $t - \alpha$ oppure $1/t$, quindi $\overline{k}(t) = \overline{k}(z)$. Ci basta verificare allora che gli elementi della forma $1/(z-\beta)$ con $\beta \in \overline{k}^*$ sono invertibili nel campo delle serie formali:

$$\frac{1}{z-\beta} = -\frac{1}{\beta}\frac{1}{1-\frac{z}{\beta}} = -\frac{1}{\beta}\sum_{i=0}^{\infty} z^i \beta^{-i}.$$

Per la seconda affermazione notiamo che $N_{\tilde{\mathfrak{P}}}$ contiene $\overline{k}(t)_{\mathfrak{P}}$, pertanto è isomorfo ad un'estensione di $\overline{k}((z))$. Nel completamento il posto $\mathfrak{P}'$ (completamento di $\mathfrak{P}$) ha una sola estensione $\tilde{\mathfrak{P}}'$ (il completamento di $\mathfrak{P}'$), quindi vi è un $v' \in \mathfrak{P}'$ tale che $v'^e = z\eta'$, con $\eta' \in \overline{k}((z))^*$ e $e := e(\tilde{\mathfrak{P}}'|\mathfrak{P}')$. L'equazione

$$\eta^e = \left(\sum_{i=0}^{\infty} \alpha_i v^i\right)^e = \eta' = \sum_{i=0}^{\infty} \alpha'_i v^i$$

ha soluzione: α_0 può essere scelto tra le radici e-esime di α'_0; per induzione, α_n va scelto in modo da soddisfare $\alpha_i \alpha_0^{e-1} = \alpha'_{ie} - f(\alpha_0, \ldots, \alpha_{i-1})$, ed esiste in quanto $\alpha_0 \neq 0$. Sostituendo quindi v' con $v := v'\eta^{-1}$ otteniamo $v^e = v'^e \eta^{-e} = z\eta'\eta'^{-1} = z$.

Dunque $N_{\tilde{\mathfrak{P}}}$ è un'estensione non ramificata di $k((v))$. Ogni suo elemento si scriverà pertanto come serie:

$$n = \sum_{i=0}^{\infty} \eta_i v^i$$

con gli η_i elementi di ordine 0. Poiché il campo residuo del posto $\tilde{\mathfrak{P}}$ è un'estensione di $\overline{k}$, gli elementi di ordine 0 sono tutti della forma $\eta = \alpha + v\eta'$, con $\alpha_i \in \overline{k}$ e η' di ordine 0. Sostituendo in ordine i coefficienti di n con coefficienti in $\overline{k}$, partendo da η_0, otteniamo che di fatto n è un elemento di $\overline{k}((v))$, quindi $N_{\tilde{\mathfrak{P}}} = \overline{k}((v))$.

Il gruppo di inerzia di $\tilde{\mathfrak{P}}$ su $\mathfrak{P}$ lascia invariati gli ordini rispetto a $\tilde{\mathfrak{P}}$ degli elementi di N e lascia fisso il campo residuo $\overline{k}$, pertanto la sua azione si estende

in modo unico su $N_{\tilde{\mathfrak{P}}}$ e manda v in ζv con ζ radice e-esima dell'unità. Per confronto dei gradi il gruppo di inerzia si mappa suriettivamente sul gruppo di Galois di $N_{\tilde{\mathfrak{P}}}/\overline{k}(t)_{\mathfrak{P}}$, quindi un generatore agisce come moltiplicazione per una radice primitiva. □

Teorema 1.44. *Sia $\overline{k}$ un sottocampo algebricamente chiuso di $\mathbb{C}$ e $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ un insieme finito di posti di $\mathbb{P}(\overline{k}(t)/\overline{k})$. Allora ogni estensione finita $N/\mathbb{C}(t)$ non ramificata fuori da S è definita su $\overline{k}(t)$. Inoltre l'estensione $N_{\overline{k}} := N_{\overline{k}(t)}$ è unica.*

Dimostrazione. Sia $N/\mathbb{C}(t)$ un'estensione finita non ramificata fuori da S. Chiamiamo Δ il gruppo degli automorfismi di $\mathbb{C}/\overline{k}$ estesi a $\overline{\mathbb{C}(t)}$ fissando l'elemento t. Supponiamo inoltre che N sia un'estensione normale; per ogni altra estensione N' basterà prendere la chiusura normale, che evidentemente sarà ramificata solo su S, e poi prendere il campo fisso del gruppo associato nella corrispondente estensione di $\overline{k}(t)$. Ipotizziamo per semplicità che S non contenga il posto infinito (basta fare un cambio di parametro $t \mapsto 1/(t-\alpha)$ con $(t-\alpha) \notin \mathfrak{P}_i$).

Consideriamo l'azione di Δ su N: poiché in ogni gruppo finitamente generato ci sono un numero finito di sottogruppi normali di indice fissato, ci possono essere solo un numero finito di possibili $\delta(N)$ al variare di $\delta \in \Delta$. Di conseguenza lo stabilizzatore Δ_N di N ha indice finito, quindi $\mathbb{C}(t)^{\Delta_N}/\overline{k}(t)$ è un'estensione finita di costanti, ma essendo $\overline{k}$ algebricamente chiuso otteniamo $\mathbb{C}^{\Delta_N} = \overline{k}$.

Scegliamo ora un posto $\mathfrak{P}_a$ di $\overline{k}$ fuori da S associato ad un punto in $a \in \overline{k}$, $\tilde{\mathfrak{P}}_a$ una sua estensione in N e studiamo l'azione di Δ_N sulle estensioni di $\mathfrak{P}_a$. Di nuovo l'orbita è necessariamente finita, quindi come sopra Δ_a (lo stabilizzatore di $\tilde{\mathfrak{P}}_a$ in Δ_N) ha indice finito in Δ_N e $\mathbb{C}^{\Delta_a} = \overline{k}$.

Sia $m_0 \geq 1$ il minimo intero per il quale esista una funzione z con polo unico in $\tilde{\mathfrak{P}}_a$ di ordine m_0; esiste sicuramente per il teorema 1.24 e sfruttando opportunamente la corrispondenza fra campi e superficie. Qualunque altra funzione z' con la stessa proprietà è della forma $\alpha z + \beta$, con $\alpha, \beta \in \mathbb{C}$: scrivendo lo sviluppo in serie di Laurent in una carta, si vede che esiste uno scalare tale per cui $\alpha z - z'$ ha polo di ordine minore di m_0 in $\tilde{\mathfrak{P}}_a$; per minimalità di m_0 $z - \alpha z'$ non ha né zeri né poli ed è quindi costante.

Inoltre $\mathfrak{P}_a$ spezza completamente in N, quindi i coniugati di z su $\mathbb{C}(t)$ hanno poli tutti distinti fra di loro e ne consegue che $N = \mathbb{C}(t, z)$.

Passiamo al completamento $N_a := N_{\tilde{\mathfrak{P}}_a}$. Sempre poiché $\mathfrak{P}_a$ non ha ramificazione, N_a è isomorfo al campo delle serie formali $\mathbb{C}((t-a))$. Qualunque funzione con polo di ordine al più m_0 in $\tilde{\mathfrak{P}}_a$ avrà sviluppo

$$\sum_{i=-m_0}^{+\infty} a_i (t-a)^i \qquad a_i \in \mathbb{C}.$$

Modifichiamo dunque z per avere $a_{-m_0} = 1$ e $a_0 = 0$ nel suo sviluppo. Facciamo ora agire Δ_a: per costruzione lascerà invariato $\tilde{\mathfrak{P}}_a$, quindi anche $(t-a)$ e la sua azione sarà determinata coefficiente per coefficiente. $\delta(z)$ è dunque una funzione con polo in $\tilde{\mathfrak{P}}_a$ di ordine m_0 e quindi della forma $bz + c$. Confrontando i coefficienti a_{-m_0} e a_0 otteniamo che in realtà $\delta(z) = z$, ovvero z è invariante per Δ_a.

In conclusione, il polinomio minimo di z su $\mathbb{C}(t)$ deve essere anche esso invariante per Δ_a, pertanto i suoi coefficienti giacciono in $\overline{k}(t)$. Di conseguenza l'estensione $\overline{k}(t,z)/\overline{k}(t)$ ha lo stesso grado di $\mathbb{C}(t,z)/\mathbb{C}(t)$, quindi è linearmente disgiunta da $\mathbb{C}(t)$. Pertanto soddisfa tutte le proprietà della definizione 1.42.

Supponiamo ora di avere due estensioni N_1, N_2 distinte finite su $\overline{k}(t)$ con $N_1\mathbb{C} = N_2\mathbb{C} = N$. Allora il grado di $N_1N_2/\overline{k}(t)$ è strettamente maggiore del grado di $N_1/\overline{k}(t) = N/\mathbb{C}(t)$; dato che N_1 e N_2 sono entrambe disgiunte da $\mathbb{C}(t)$ questo implica che $N_1N_2\mathbb{C}/\mathbb{C}(t)$ abbia anch'essa grado maggiore di $N/\mathbb{C}(t)$, contraddicendo l'ipotesi. □

Col teorema appena visto si stabilisce quindi una corrispondenza biunivoca tra estensioni di $\mathbb{C}$ e di $\overline{k}$ ramificate solo in un insieme finito S definito su $\overline{k}$, e tale corrispondenza rispetta intersezioni e composizioni. È quindi immediato trasferire i teoremi 1.40 e 1.41:

Teorema 1.45 (RET profinito su $\overline{k}$)**.** *Sia S un insieme finito di posti di $\overline{k}(t)$ e $\tilde{S}$ il corrispondente insieme di punti di $\mathbb{P}^1(\overline{k})$. Chiamiamo N_S l'estensione massima di $\overline{k}(t)$ in una chiusura algebrica $\overline{\overline{k}(t)}$ che sia ramificata solo in S; allora vale:*

$$\mathrm{Gal}(N_S/\overline{k}(t)) \cong \Gamma_s.$$

Teorema 1.46. *Sia $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ un insieme di posti di $\overline{k}(t)$ e siano γ_i i rispettivi generatori di Γ_s. Esistono allora delle estensioni $\overline{\mathfrak{P}}_i$ dei posti in N_S tali per cui:*

$$\forall 1 \le i \le n \quad \overline{\langle \gamma_i \rangle} = I(\overline{\mathfrak{P}}_i/\mathfrak{P}_i).$$

Quest'ultimo risultato può essere anche raffinato in vista del lemma 1.43.

Teorema 1.47. *Sia $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ un insieme di posti di $\overline{k}(t)$. I generatori γ_i del teorema 1.46 possono essere scelti in modo che in ogni estensione normale finita $N/\mathbb{Q}(t)$ ramificata in S la loro azione sui completamenti sia determinata dalla moltiplicazione del parametro locale per ζ_e, dove e è l'indice di ramificazione.*

Dimostrazione. Prendiamo un posto $\overline{\mathfrak{P}}$ sopra $\mathfrak{P} := \mathfrak{P}_i$ e sia γ' un generatore del gruppo di inerzia $I(\overline{\mathfrak{P}}|\mathfrak{P})$; sia anche z un parametro locale per $\mathfrak{P}$.

Fissiamo un'estensione normale N finita su $\mathbb{Q}(t)$; in essa γ' è un generatore del gruppo di inerzia, pertanto nel completamento agirà come moltiplicazione per ζ_e^k con $k \in (\mathbb{Z}/e\mathbb{Z})^*$. Sia $k(N)$ la funzione che associa alle estensioni normali il corrispondente esponente in $(\mathbb{Z}/e_N\mathbb{Z})^*$, dove e_N è l'indice di ramificazione di $\overline{\mathfrak{P}}$ ristretto a N. Verifichiamo ora che $k(N)$ è ben definito e identifica un elemento $\hat{k} \in \hat{\mathbb{Z}}^*$.

Innanzitutto, se v e v' sono due parametri locali per cui $N_{\mathfrak{P}} = \overline{\mathbb{Q}}((v)) = \overline{\mathbb{Q}}((v'))$, allora $v' = \zeta v$ per ζ radice dell'unità. L'azione di γ_i di conseguenza è ζ_e^k con lo stesso k in entrambi i casi, per cui $k(N)$ è ben definito.

Date due estensioni normali di grado finito $N_1/\overline{\mathbb{Q}}(t)$ e $N_2/\overline{\mathbb{Q}}(t)$ prendiamo $N_3 := N_1N_2$, che sarà normale e finita su $\overline{\mathbb{Q}}(t)$. Siano $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ le rispettive restrizioni di $\overline{\mathfrak{P}}$. Allora i completamenti $(N_1)_{\mathfrak{P}_1}$ e $(N_2)_{\mathfrak{P}_2}$ saranno contenuti in

$(N_3)_{\mathfrak{P}_3}$. Chiamando v_1, v_2, v_3 i rispettivi parametri locali e e_1, e_2, e_3 gli indici di ramificazione abbiamo

$$v_3^{e_3/e_1} = \zeta v_1, \quad v_3^{e_3/e_2} = \zeta' v_2$$

poiché vale $v_i^{e_i} = z$. Allora evidentemente $k(N_3) \equiv k(N_i) \mod e_i$ per $i = 1, 2$.

Inoltre esistono estensioni con tutti gli indici di ramificazione possibili (basta prendere i polinomi $x^e = z$). Quindi $k(N)$ passa al limite profinito e definisce un elemento $\hat{k} \in \hat{\mathbb{Z}}^*$.

Basta ora sostituire γ' con $\gamma := \gamma^{\hat{k}^{-1}}$ per ottenere il generatore desiderato. □

Capitolo 2

Rigidità

2.1 Il carattere ciclotomico

Chiamiamo d'ora in poi N_S l'estensione algebrica massima di $\overline{\mathbb{Q}}(t)$ ramificata solo in S, con S insieme finito di posti di $\overline{\mathbb{Q}}(t)$, e Γ_s il gruppo di Galois associato in cui vi sia la corrispondenza esposta fra generatori e gruppi di inerzia degli elementi di S. Sia inoltre $\Gamma_{\mathbb{Q}}$ il gruppo di Galois assoluto di $\overline{\mathbb{Q}}$, ovvero $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Identificheremo d'ora in poi liberamente $\Gamma_{\mathbb{Q}}$ e $\mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$.

Teorema 2.1 (Teorema di spezzamento)**.** *Sia S un insieme di posti in $\mathbb{P}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}})$ invariante per l'azione di $\Gamma_{\mathbb{Q}}$. Allora N_S è di Galois su $\mathbb{Q}(t)$ e vale la fattorizzazione*

$$\mathrm{Gal}(N_S/\mathbb{Q}(t)) \cong \Gamma_s \rtimes \Gamma_{\mathbb{Q}}. \tag{2.1.1}$$

I complementari di Γ_s possono essere scelti tra i gruppi di decomposizione di posti di grado uno in $\mathbb{P}(\mathbb{Q}(t)/\mathbb{Q})$ non ramificati in N_S.

Dimostrazione. N_S è certamente algebrica su $\mathbb{Q}$; ogni sua immersione in una chiusura algebrica $\overline{N_S}$ permuta gli elementi di S, pertanto, in quanto estensione massima ramificata in S, resta invariante e quindi è di Galois.

Ora sia $\mathfrak{P}$ un posto di $\mathbb{P}(\mathbb{Q}(t)/\mathbb{Q})$ di grado uno che si estenda ad un $\overline{\mathfrak{P}}$ non ramificato in N_S. Gli elementi Γ_s permutano fedelmente le estensioni di $\mathfrak{P}$, poiché non ha ramificazione su $\overline{\mathbb{Q}}(t)$ e quindi spezza completamente, pertanto il suo gruppo di decomposizione su $\mathbb{Q}(t)$ ha intersezione banale con Γ_s; la sua proiezione al quoziente per Γ_s, invece, è il gruppo di decomposizione da $\overline{\mathbb{Q}}(t)$ a $\mathbb{Q}(t)$, ma essendo $\mathfrak{P}$ di grado 1 questo è tutto $\Gamma_{\mathbb{Q}}$.

Il gruppo di decomposizione di $\mathfrak{P}$ è quindi un complementare di Γ_s e vale la fattorizzazione cercata. □

L'azione di $\Gamma_{\mathbb{Q}}$ su Γ_s non è nota esplicitamente, ma alcune informazioni sono ricavabili dall'azione sulle radici dell'unità. Diamo quindi la seguente definizione:

Definizione 2.2. Si dice *carattere ciclotomico* la funzione

$$c : \Gamma_{\mathbb{Q}} \to \hat{\mathbb{Z}}^*, \quad \delta \to c(\delta) = (c_n(\delta))_{n\in\mathbb{N}}$$

dove $c_n(\delta) \in (\mathbb{Z}/n\mathbb{Z})^*$ è l'esponente tale per cui $\delta(\zeta_n) = \zeta_n^{c_n(\delta)}$.

Proposizione 2.3. *Il carattere ciclotomico è ben definito ed è un isomorfismo fra* Γ_s^{ab} *e* $\hat{\mathbb{Z}}^*$.

Dimostrazione. Il carattere ciclotomico è evidentemente ben definito: se $m \mid n$ allora $\zeta_m^{c_m(\delta)} = \delta(\zeta_m) = \delta(\zeta_n^{n/m}) = \zeta_n^{c_n(\delta)n/m}$. Quindi $c_m(\delta) \equiv_m c_n(\delta)$.

Il campo fisso di $\ker(c)$ è l'estensione di $\mathbb{Q}$ generata dalle radici dell'unità; per il teorema di Kronecker-Weber questa estensione contiene tutte le estensioni abeliane, nonché è abeliana anche essa in quanto composizione di estensioni abeliane disgiunte. Di conseguenza $\Gamma_{\mathbb{Q}}/\ker(c)$ si mappa surgettivamente su tutti i quozienti abeliani di $\Gamma_{\mathbb{Q}}$, ovvero è $\Gamma_{\mathbb{Q}}^{\mathrm{ab}}$. □

Se ci rimettiamo nelle ipotesi del teorema 2.1, ovvero che S sia invariante per $\Gamma_{\mathbb{Q}}$, e chiamiamo i^δ l'intero per cui si abbia $\delta(\mathfrak{P}_i) = \mathfrak{P}_{i^\delta}$ per i posti di S, possiamo ricavare l'azione di $\Gamma_{\mathbb{Q}}$ sulle classi di coniugio dei generatori γ_i di Γ_s.

Teorema 2.4. *Sia S un insieme di posti di $\overline{\mathbb{Q}}(t)$ invariante per l'azione di $\Gamma_{\mathbb{Q}}$, Δ un complementare chiuso di Γ_s in $\mathrm{Gal}(N_S/\mathbb{Q}(t))$ e siano γ_i i generatori di Γ_s associati ai posti secondo le convenzioni stabilite.*

Identificando Δ con $\Gamma_{\mathbb{Q}}$ otteniamo che per ogni $\delta \in \Gamma_{\mathbb{Q}}$ vale

$$[\gamma_i^\delta] = [\gamma_{i^\delta}^{c(\delta)}]$$

dove $[\gamma]$ indica la classe di coniugio di γ in Γ_s.

Dimostrazione. Mettiamoci in una sottoestensione N normale su $\mathbb{Q}(t)$ e finita su $\overline{\mathbb{Q}}(t)$; sia $\tilde{\mathfrak{P}}_i$ un'estensione di $\mathfrak{P}_i$ tale per cui la restrizione $\tilde{\gamma}_i$ generi il gruppo di inerzia su $\overline{\mathbb{Q}}(t)$. Il teorema 1.47 afferma allora che $\tilde{\gamma}_i$ agisce sul completamento $N_{\tilde{\mathfrak{P}}_i} = \overline{\mathbb{Q}}((v_i))$ moltiplicando il parametro locale v_i per la radice dell'unità ζ_e, con e indice di ramificazione. Fissiamo ora i parametri locali $z_i \in \mathfrak{P}_i$ in modo che siano coniugati fra di loro per l'azione di $\Gamma_{\mathbb{Q}}$ e stabiliamo per $\tilde{\mathfrak{P}}_i$ un parametro locale v_i nel completamento con $v_i^e = z_i$; chiamiamo $\overline{\gamma}_i$ le azioni indotte dai $\tilde{\gamma}_i$. Fissati $\tilde{\mathfrak{P}}_{i^\delta} := \delta(\tilde{\mathfrak{P}}_i)$, $\tilde{\gamma}_{i^\delta}$ un generatore del gruppo di inerzia di $\tilde{\mathfrak{P}}_{i^\delta}$ e v'_{i^δ} un parametro locale del completamento rispetto a $\mathfrak{P}_{i^\delta}$, qualsiasi $\delta \in \Gamma_{\mathbb{Q}}$ si estende in modo unico ad una mappa

$$\begin{aligned} \hat{\delta} : N_{\tilde{\mathfrak{P}}_i} &\to N_{\tilde{\mathfrak{P}}_{i^\delta}} \\ z_i &\mapsto \delta(z_i) = z_{i^\delta} \\ \alpha \in \overline{\mathbb{Q}} &\mapsto \delta(\alpha) \end{aligned}$$

pertanto deve valere

$$v_i \in \overline{\mathbb{Q}} \mapsto \zeta v_{i^\delta}.$$

Calcoliamo infine

$$(\overline{\delta} \circ \overline{\gamma}_i)(v_i) = \overline{\delta}(\zeta_e v_i) = \zeta_e^{c_e(\delta)} \zeta v_{i^\delta} = \overline{\gamma}_{i^\delta}^{c_e(\delta)}(\zeta v_{i^\delta}) = (\overline{\gamma}_{i^\delta}^{c_e(\delta)} \circ \overline{\delta})(v_i).$$

Restringendo le mappe $\overline{\gamma}_i$ e $\overline{\delta}$ a N otteniamo $\delta \circ \tilde{\gamma}_i = \tilde{\gamma}_{i^\delta}^{c_e(\delta)} \circ \delta$, ossia $\tilde{\gamma}_i^\delta = \tilde{\gamma}_{i^\delta}^{c_e(\delta)}$.

Ricordando ora che i possibili $\tilde{\gamma}_i$ sono coniugati fra di loro tramite Γ_s, pertanto anche tramite $\mathrm{Gal}(N/\overline{\mathbb{Q}}(t))$, otteniamo

$$[\tilde{\gamma}_i^\delta] = [\tilde{\gamma}_{i^\delta}^{c_e(\delta)}]$$

con $[\tilde{\gamma}]$ classe di coniugio di $\tilde{\gamma}$ in $\mathrm{Gal}(N/\overline{\mathbb{Q}}(t))$.

Per passare al completamento profinito osserviamo che ogni estensione normale $N/\overline{\mathbb{Q}}(t)$ ramificata solo in S ha chiusura normale su $\mathbb{Q}(t)$ di grado finito su $\overline{\mathbb{Q}}(t)$; infatti il polinomio che genera N ha un numero finito di coefficienti, pertanto un numero finito di coniugati possibili su $\mathbb{Q}(t)$, e componendo tutte le estensioni generate dai polinomi coniugati otteniamo un'estensione normale su $\mathbb{Q}(t)$ di grado finito su $\overline{\mathbb{Q}}(t)$. Possiamo quindi passare al limite e ottenere l'equazione desiderata. □

2.2 Campi di definizione

Dobbiamo ora cercare di trasferire le estensioni di $\overline{\mathbb{Q}}(t)$ su campi più piccoli, possibilmente su $\mathbb{Q}(t)$. Cerchiamo dunque delle condizioni per cui un sottocampo soddisfi la definizione 1.42.

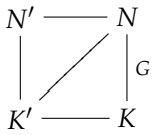
Proposizione 2.5. *Sia N/K un'estensione di Galois con gruppo G e K' un suo campo di definizione su cui K è di Galois. Allora anche N/K' è di Galois e si ha*

$$\mathrm{Gal}(N/K') \cong \mathrm{Gal}(N/K) \rtimes \mathrm{Gal}(K/K').$$

Se K' è anche campo di definizione con G il prodotto sopra indicato è diretto.

Dimostrazione. Sia N' l'estensione di K' disgiunta da K/K' e per cui si abbia $N'K = N$. Gli automorfismi di K/K' si sollevano in modo unico a N/N' e viceversa gli automorfismi di N/N' si restringono a K, pertanto si ha $\mathrm{Gal}(N/N') \cong \mathrm{Gal}(K/K')$.

Il gruppo di automorfismi generato da $\mathrm{Gal}(N/K)$ e $\mathrm{Gal}(N/N')$ ha campo fisso $N' \cap K$, ovvero K' stesso, di conseguenza N/K' è di Galois. Inoltre per corrispondenza di Galois $\mathrm{Gal}(N/K) \cap \mathrm{Gal}(N/N') = \{e\}$, ed essendo N/N' normale il sottogruppo associato è normale e otteniamo la fattorizzazione indicata.

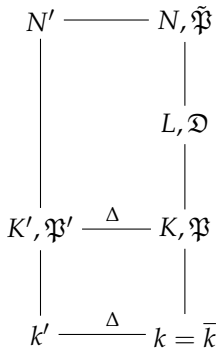


Se il campo K' è anche di definizione per G abbiamo che N'/K' è normale, quindi $\mathrm{Gal}(N/N')$ è normale e deve commutare con G. Il prodotto è pertanto diretto. □

Facciamo ora un'ipotesi che nei casi da noi studiati sarà sempre verificata, ovvero che in K esista sempre un posto di grado 1.

Definizione 2.6. Un campo K si dice *dischiuso* se possiede un posto di grado uno.

Teorema 2.7. *Sia $K/k(t)$ un'estensione algebrica con k algebricamente chiuso e N/K un'estensione finita di Galois. Un sottocampo dischiuso K' di K tale che $kK' = K$ è di definizione per N/K se e solo se N/K' è di Galois.*



Dimostrazione. Un'implicazione ci è data dalla proposizione 2.5. Supponiamo ora che N/K' sia di Galois. Chiamiamo $k' = K' \cap k$, Δ il gruppo $\mathrm{Gal}(K/K')$ che sarà isomorfo a per ipotesi a $\mathrm{Gal}(k/k')$, $\mathfrak{P}'$ un posto di K' di grado uno e $\tilde{\mathfrak{P}}$, $\mathfrak{P}$ delle sue estensioni compatibili a N e K rispettivamente.

Sia L il campo di inerzia di $\tilde{\mathfrak{P}}/\mathfrak{P}$ e $\mathfrak{D}$ la restrizione di $\tilde{\mathfrak{P}}$ in tale campo. Gli automorfismi che non lasciano fisso K agiscono in modo non banale su k; ma quest'ultimo è isomorfo al campo residuo di $\mathfrak{P}$ compatibilmente con l'azione di Galois per l'ipotesi sul grado, quindi in particolare gli automorfismi detti non appartengono al gruppo di inerzia. Questo implica $K \subset L$.

L'estensione $\mathfrak{D}/\mathfrak{P}'$ non è ramificata; scegliamo quindi un elemento $z \in K'$ che sia parametro locale in $\mathfrak{P}'$ e il completamento $L_{\mathfrak{D}}$ sarà isomorfo a $k((z))$ e $N_{\tilde{\mathfrak{P}}}$ isomorfo a $k((y))$, dove $y^{e(\tilde{\mathfrak{P}}/\mathfrak{D})} = z$. Un qualsiasi automorfismo $\delta \in \Delta$ agisce su $k((z))$ coefficiente per coefficiente, pertanto possiamo estenderlo in modo unico a $\hat{\delta}$ su $k((y))$ in modo che fissi y. Definiamo ora il seguente gruppo:

$$\tilde{\Delta} = \{\tilde{\delta} \mid \tilde{\delta} \equiv \hat{\delta}|_N,\ \delta \in \Delta\}.$$

Questo è un sottogruppo chiuso di $\mathrm{Gal}(N/K')$ isomorfo a Δ con la proprietà aggiuntiva di essere complementare a $\mathrm{Gal}(N/K)$. Di conseguenza $N' = N^{\tilde{\Delta}}$ è un'estensione di K' linearmente disgiunta da K e per cui si ha $N'K = N$, quindi N/K è definito su K'. □

L'estensione appena ottenuta non è di Galois, pertanto non è sufficiente a darci una realizzazione del gruppo G su K'. Cerchiamo allora delle condizioni per cui K' è anche di definizione per G.

Proposizione 2.8. *Sia N/K un'estensione finita di Galois gruppo di automorfismi G e campo di definizione K' sul quale N è normale. Allora K è anche di definizione per $N/_G K$ se e solo se gli elementi di* $\mathrm{Inn}(\mathrm{Gal}(N/K'))$ *agiscono su G come* $\mathrm{Inn}(G)$ *e il centro di G ha complementare chiuso nel centralizzatore $\mathcal{C}_{\mathrm{Gal}(N/K')}(G)$.*

Dimostrazione. Chiamiamo $\Gamma = \mathrm{Gal}(N/K')$. Se K' è di definizione per $N/_G K$ la fattorizzazione della proposizione 2.5 fornisce un complementare Δ di G in Γ; esso è anche un complementare per $Z(G)$ in $\mathcal{C}_\Gamma(G) = \Delta \times Z(G)$. Dato che G è un fattore diretto, gli elementi di $\mathrm{Inn}(\Gamma)$ agiscono su G solo tramite la componente in G, quindi come $\mathrm{Inn}(G)$.

Viceversa, prendiamo un qualsiasi $\gamma \in \Gamma$ e chiamiamo g il corrispondente elemento di G che ne esprime l'azione, ovvero $\gamma h \gamma^{-1} = ghg^{-1}$ per ogni $h \in G$. Scrivendola come $g^{-1}\gamma h = hg^{-1}\gamma$ ricaviamo immediatamente $\gamma \in g\,\mathcal{C}_\Gamma(G)$, quindi G e $\mathcal{C}_\Gamma(G)$ generano tutto il gruppo. Il complementare Δ di $Z(G)$ in $\mathcal{C}_\Gamma(G)$ è quindi complementare di G in Γ ed è contenuto nel suo centralizzatore, pertanto $\Gamma \cong \Delta \times G$. Il suo campo fisso è un'estensione normale di K' invariante per l'azione di G che quindi soddisfa la definizione 1.42. □

Forniamo ora, dopo un lemma di teoria dei gruppi, una condizione sufficiente per il verificarsi delle ipotesi appena richieste.

Lemma 2.9. *Sia G un gruppo, H un suo sottogruppo contenente $Z(G)$ e Γ il prodotto semidiretto $G \rtimes H/Z(G)$ in cui si considera l'azione di coniugio. Se H possiede un complementare per $Z(G)$ allora*

$$\mathcal{C}_\Gamma(G) \cong H$$

e l'isomorfismo manda $(g, e) \mapsto g$ per tutti gli elementi $g \in Z(G)$.

Dimostrazione. Calcoliamo il centralizzatore:

$$\begin{aligned}
\mathcal{C}_\Gamma(G) &= \{(g,\overline{h}) \mid (g,\overline{h}) \cdot (l,e) \cdot (g,\overline{h})^{-1} = (l,e) \quad \forall l \in G\} \\
&= \{(g,\overline{h}) \mid (g,\overline{h}) \cdot (l,e) \cdot (h^{-1}gh, \overline{h}^{-1}) = (l,e) \quad \forall l \in G\} \\
&= \{(g,\overline{h}) \mid (ghlh^{-1}, \overline{h}) \cdot (h^{-1}g^{-1}h, \overline{h}^{-1}) = (l,e) \quad \forall l \in G\} \\
&= \{(g,\overline{h}) \mid (ghlh^{-1}hh^{-1}g^{-1}hh^{-1}, \overline{hh^{-1}}) \quad \forall l \in G\} \\
&= \{(g,\overline{h}) \mid (ghlh^{-1}g^{-1}, e) = (l,e) \quad \forall l \in G\} \\
&= \{(g,\overline{h}) \mid ghl = lgh \quad \forall l \in G\} \\
&= \{(g,\overline{h}) \mid gh \in Z(G)\}.
\end{aligned}$$

Sia M il complementare di $Z(G)$ in H. Allora per ogni $h \in H$ esiste un unico $h_m \in M$ e un $z \in Z(G)$ per cui $h = h_m z$, pertanto $hZ(G) = h_m z Z(G) = h_m Z(G)$. Riscriviamo allora

$$\mathcal{C}_\Gamma(G) = \{(g,\overline{h}_m) \mid gh_m \in Z(G),\ h_m \in M\}.$$

e costruiamo la funzione:

$$\begin{aligned}
\phi : \mathcal{C}_\Gamma(G) &\longrightarrow Z(G) \times H' \\
(g,\overline{h}) &\mapsto (gh_m, h_m)
\end{aligned}$$

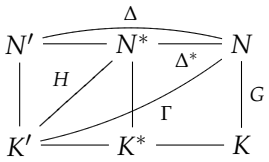
che è un omomorfismo:

$$\begin{aligned}
\phi(g,\overline{h}) \cdot (g',\overline{h'}) &= \phi(gh_m g' h_m^{-1}, \overline{h_m h'_m}) \\
&= \phi(g'g, \overline{h_m h'_m}) = (g'gh_m h'_m, h_m h'_m) \\
&= (gh_m g' h'_m, h_m h'_m) = (gh_m, h_m) \cdot (g' h'_m, h'_m) \\
&= \phi(g,\overline{h})\phi(g',\overline{h'}).
\end{aligned}$$

Dato che esiste un unico h_m per ogni classe $\overline{h}$ e che $gh_m = e$ implica $g = h_m = e$, poiché $M \cap Z(G) = \{e\}$, ϕ è anche un isomorfismo. Quindi $\mathcal{C}_\Gamma(G) \cong Z(G) \times M \cong H$.

Per l'ultima affermazione basta osservare che $\phi(g,\overline{e}) = (g,e)$, con $g \in Z(G)$, e che l'isomorfismo tra $Z(G) \times M$ e H manda proprio $(Z(G), e)$ in $Z(G)$. □

Teorema 2.10. *Sia N/K un'estensione di Galois con le stesse ipotesi del teorema 2.7. Supponiamo anche che ogni elemento di $\mathrm{Gal}(N/K')$ agisca come un automorfismo interno su G e che esista un posto $\mathfrak{P}'$ di grado uno in K' per cui il centro di G abbia un complementare in $\mathcal{N}_G(I(\tilde{\mathfrak{P}}/\mathfrak{P}))$, dove $\tilde{\mathfrak{P}}$ è un'estensione di $\mathfrak{P}'$ a N e $\mathfrak{P}$ la restrizione a K. Allora K' è anche campo di definizione di $N/_G K$.*



Dimostrazione. Nella dimostrazione del teorema 2.7abbiamo costruito un gruppo Δ all'interno del gruppo di decomposizione $D(\tilde{\mathfrak{P}}|\mathfrak{P}')$. Chiamiamo ora $\Delta^* = \Delta \cap \mathcal{C}_\Gamma(G)$, N^* il suo campo fisso e K^* la rispettiva intersezione con K; tale sottogruppo è normale in Δ in quanto lo è $\mathcal{C}_\Gamma(C)$, mentre commuta con G, quindi è normale in Γ. Chiamiamo infine H il gruppo $\mathrm{Gal}(N^*/K')$ e osserviamo che è isomorfo a $G \rtimes \Delta/\Delta^*$; per costruzione Δ agisce su G come $\mathrm{Inn}(G)$, quindi quozientando per gli elementi che commutano con G abbiamo che H si immerge in $G \rtimes \mathrm{Inn}(G)$.

Ogni elemento di Δ ha la proprietà di lasciare invariato, agendo su G, il gruppo di decomposizione $D(\tilde{\mathfrak{P}}|\mathfrak{P}) = I(\tilde{\mathfrak{P}}|\mathfrak{P})$ (il campo k è algebricamente chiuso, per cui non vi può essere inerzia). Di conseguenza i corrispondente automorfismi in $\mathrm{Inn}(G)$ saranno rappresentati da elementi di $\mathcal{N}_G(G_I)$. Questa proprietà si trasferisce ovviamente su $\mathrm{Gal}(N^*/N') = \Delta/\Delta^*$. Se chiamiamo M il sottogruppo di $\mathcal{N}_G(G_I)$ formato dagli elementi che nel coniugio agiscono come elementi di Δ, vale $Z(G) < M$ e $\Delta/\Delta^* \cong M/Z(G)$; inoltre il centro possiede, per ipotesi, complementare in $\mathcal{N}_G(G_I)$ e quindi anche in M. Inoltre $M/Z(G)$ è un sottogruppo di $\mathrm{Inn}(G) = G/Z(G)$ corrispondente all'azione di Δ, pertanto isomorfo a Δ/Δ^*.

Applicando il lemma precedente a G e M otteniamo che $\mathcal{C}_{G\rtimes M/Z(G)}(G)$ è isomorfo a M. $M/Z(G)$ è però isomorfo a Δ/Δ^*, quindi otteniamo $M \cong \mathcal{C}_H(G)$. Dunque $\mathcal{C}_H(G)$ possiede un complementare di $Z(G)$, per cui si applica la proposizione 2.8 all'estensione N^*/K' e otteniamo un'estensione N''/K' di Galois che soddisfi le proprietà che ci servono. □

2.3 Rigidità debole

Ora che abbiamo preparato alcuni strumenti per cambiare campo base delle estensioni di $\overline{\mathbb{Q}}(t)$, tentiamo di classificare queste ultime sulla base di sole proprietà algebriche del gruppo di Galois associato. Dallo studio di questa classificazione ricaveremo poi i criteri detti di "rigidità".

Teorema 2.11 (Classificazione di Hurwitz)**.** *Definiamo i seguenti oggetti:*

$$\begin{gathered} E_S(G) := \{N \mid \overline{\mathbb{Q}}(t) \subset N \subset N_S, \mathrm{Gal}(N/\overline{\mathbb{Q}}(t)) \cong G\} \\ \Sigma_s(G) := \{\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_s) \mid \langle \boldsymbol{\sigma} \rangle = G, \sigma_1 \cdots \sigma_s = e\} \\ \psi_{\boldsymbol{\sigma}} : \Gamma_s \to G, \\ \psi_{\boldsymbol{\sigma}}(\gamma_i) = \sigma_i \\ \ker(\boldsymbol{\sigma}) = \ker(\psi_{\boldsymbol{\sigma}}),\ N_{\boldsymbol{\sigma}} = N_S^{\ker(\boldsymbol{\sigma})}. \end{gathered}$$

La seguente mappa

$$\begin{array}{rccc} H_S : & \Sigma_s(G)/\operatorname{Aut}(G) & \to & E_S(G) \\ & \boldsymbol{\sigma}^{\operatorname{Aut}(G)} & \to & N_{\boldsymbol{\sigma}} \end{array}$$

è una bigezione. Le componenti σ_i di $\boldsymbol{\sigma}$ forniscono i generatori dei gruppi di inerzia

dei posti $\mathfrak{P}_i$ tramite

$$\varphi_{\boldsymbol{\sigma}} : G \to \mathrm{Gal}(N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t)),\ \sigma_i \to \psi_{\boldsymbol{\sigma}}^{-1}(\sigma_i)\ker(\boldsymbol{\sigma}).$$

Dimostrazione. Siano $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \Sigma_s(G)$. Se $N_{\boldsymbol{\sigma}} = N_{\boldsymbol{\tau}}$ allora $\ker(\boldsymbol{\sigma}) = \ker(\boldsymbol{\tau})$ da cui deduciamo che $\varphi_{\boldsymbol{\sigma}}$ e $\varphi_{\boldsymbol{\tau}}$ inducono un isomorfismo tra $\Gamma/\ker(\boldsymbol{\sigma})$ e G; da questo discende che esiste un automorfismo $\alpha \in \mathrm{Aut}(G)$ per il quale $\alpha \circ \varphi_{\boldsymbol{\sigma}} = \varphi_{\boldsymbol{\tau}}$. In particolare allora avremo che $\boldsymbol{\sigma}^{\alpha} = \boldsymbol{\tau}$.

Se viceversa esiste un automorfismo tale per cui $\boldsymbol{\sigma}^{\alpha} = \boldsymbol{\tau}$ vale l'uguaglianza $\varphi_{\boldsymbol{\tau}} = \alpha \circ \varphi_{\boldsymbol{\sigma}}$, dalla quale deduciamo l'uguaglianza dei kernel e quindi dei campi fissi associati. La mappa H_S è pertanto iniettiva.

D'altra parte ad una qualsiasi estensione $N \in E_S(G)$ è associato un sottogruppo chiuso $\Psi \leq \Gamma_s$ per cui $G \cong \Gamma_s/\Psi$; la proiezione canonica sceglie un vettore $\boldsymbol{\sigma} = (\overline{\gamma_1}, \ldots, \overline{\gamma_s})$ di generatori in $\Sigma_s(G)$ per cui si abbia $N_{\boldsymbol{\sigma}} = N$. Quindi H_S è anche surgettiva.

L'affermazione sui gruppi di inerzia discende direttamente dal teorema 1.47. □

Consideriamo ora la fattorizzazione (2.1.1); ogni $\tilde{\delta}$ di un complementare $\tilde{\Gamma}_{\mathbb{Q}}$ di Γ_s isomorfo a $\Gamma_{\mathbb{Q}}$ agisce su $\mathrm{Hom}(\Gamma_s, G)$ a destra:

$$\begin{array}{rcl} \mathrm{Hom}(\Gamma_s, G) \times \tilde{\Gamma}_{\mathbb{Q}} & \to & \mathrm{Hom}(\Gamma_s, G) \\ (\psi, \tilde{\delta}) & \to & \psi.\tilde{\delta} \quad \text{con } (\psi.\tilde{\delta})(\gamma) = \psi(\tilde{\delta}\gamma\tilde{\delta}^{-1}). \end{array}$$

L'azione si trasferisce naturalmente su $\Sigma_s(G)$:

$$(\boldsymbol{\sigma}, \tilde{\delta}) \to \boldsymbol{\sigma}.\tilde{\delta} = \boldsymbol{\sigma}^{\tilde{\delta}^{-1}} \quad \text{con } \boldsymbol{\sigma}^{\tilde{\delta}} = \psi_{\boldsymbol{\sigma}}(\gamma^{\tilde{\delta}}). \tag{2.3.2}$$

Accade ora che due sollevamenti di uno stesso $\delta \in \Gamma_{\mathbb{Q}}$ in due complementari di Γ_s differiscano per un elemento di Γ_s, quindi l'azione su $\Sigma_s(G)$ definisce un'azione di $\Gamma_{\mathbb{Q}}$ su $\Sigma_s(G)/\mathrm{Inn}(G)$ e possiamo porre:

$$([\boldsymbol{\sigma}], \tilde{\delta}) \to [\boldsymbol{\sigma}].\tilde{\delta} = [\boldsymbol{\sigma}]^{\delta^{-1}} \quad \text{con } [\boldsymbol{\sigma}]^{\delta} = [\boldsymbol{\sigma}^{\tilde{\delta}}].$$

Proposizione 2.12. *Siano $\delta \in \Gamma_{\mathbb{Q}}$, $[\boldsymbol{\sigma}] \in \Sigma_s(G)/\mathrm{Inn}(G)$ e C_i le classi di coniugio delle componenti di un rappresentante $\boldsymbol{\sigma}$. Vale la formula:*

$$C_i^{\delta} = C_{i^{\delta}}^{c(\delta)}$$

Dimostrazione. Basta effettuare il calcolo e applicare il teorema 2.4:

$$C_i^{\delta} = [\sigma_i^{\tilde{\delta}}] = [\psi_{\boldsymbol{\sigma}}(\gamma_i)^{\tilde{\delta}}] = [\psi_{\boldsymbol{\sigma}}(\gamma_{i^{\delta}}^{c(\delta)})] = [\sigma_{i^{\delta}}^{c(\delta)}] = C_{i^{\delta}}^{c(\delta)}.$$

□

Nell'ipotesi in cui S sia un insieme fissato da $\Gamma_{\mathbb{Q}}$ abbiamo che le classi di coniugio vengono mappate simultaneamente nelle loro potenze: $C_i^{\delta} = C_i^{c(\delta)}$. $\Gamma_{\mathbb{Q}}$ agisce quindi come gruppo di permutazione sull'insieme

$$\mathbf{C}^* := \{\mathbf{C}^n \mid n \in (\mathbb{Z}/|G|\mathbb{Z})^*\}$$

definito per i vettori $\mathbf{C} = (C_1, \ldots, C_s) \in \mathrm{Cl}(G)^s$. L'azione è transitiva poiché il carattere ciclotomico è surgettivo su $\hat{\mathbb{Z}}^*$.

Definizione 2.13. Si chiama *grado di irrazionalità* $d(\mathbf{C})$ la cardinalità di $\mathbf{C}^*$.
Un vettore $\mathbf{C}$ con $d(\mathbf{C}) = 1$ verrà detto *razionale*.

Chiamiamo ora $\Gamma_{\mathbf{C}}$ lo stabilizzatore del vettore $\mathbf{C}$ per l'azione di $\Gamma_{\mathbb{Q}}$ e calcoliamone il campo fisso.

Proposizione 2.14. *Sia* $\mathbf{C} = (C_1, \ldots, C_s) \in \mathrm{Cl}(G)^s$ *un vettore di classi di* G*. Il campo fisso* $\mathbb{Q}_{\mathbf{C}} := \overline{\mathbb{Q}}^{\Gamma_{\mathbf{C}}}$ *è abeliano di grado* $d(\mathbf{C})$ *su* $\mathbb{Q}$*.*

Dimostrazione. L'azione di $\Gamma_{\mathbb{Q}}$ è fattorizzata tramite il carattere ciclotomico, pertanto il quoziente $\Gamma_{\mathbb{Q}}/\Gamma_{\mathbf{C}}$ sarà isomorfo ad un quoziente di $c(\Gamma_{\mathbb{Q}}) = \hat{\mathbb{Z}}^*$ che è abeliano. Il suo grado è uguale all'indice di $\Gamma_{\mathbf{C}}$ in Γ; ma essendo l'azione di $\Gamma_{\mathbb{Q}}$ transitiva su $\mathbf{C}^*$ esso è uguale al numero di elementi nell'unica orbita, ossia $d(\mathbf{C})$. □

Consideriamo ora invece lo stabilizzatore $\Gamma_{\boldsymbol{\sigma}}$ dell'azione di $\Gamma_{\mathbb{Q}}$ sull'insieme $\Sigma_s(G)/\operatorname{Inn}(G)$.

Definizione 2.15. Definiamo l'insieme

$$\Sigma(\mathbf{C}) := \{\boldsymbol{\sigma} \in \Sigma_s(G) \mid \sigma_i \in C_i\}$$

e la quantità

$$l(\mathbf{C}) := |\Sigma(\mathbf{C})/\operatorname{Inn}(G)|.$$

Un vettore $\mathbf{C}$ è detto *rigido* se $l(\mathbf{C}) = 1$.

Teorema 2.16. *Sia* G *un gruppo finito e* $\boldsymbol{\sigma} \in \Sigma(\mathbf{C})$ *un sistema di generatori. Se l'insieme dei posti ramificati* S *di* $N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t)$ *è fissato da* $\Gamma_{\mathbb{Q}}$*, il campo fisso* $k_{\boldsymbol{\sigma}} := \overline{\mathbb{Q}}^{\Gamma_{\boldsymbol{\sigma}}}$ *contiene* $\mathbb{Q}_{\mathbf{C}}$ *e vale la relazione*

$$[k_{\boldsymbol{\sigma}} : \mathbb{Q}_{\mathbf{C}}] \leq l(\mathbf{C}).$$

Dimostrazione. $\Gamma_{\boldsymbol{\sigma}}$ è evidentemente un sottogruppo di $\Gamma_{\mathbf{C}}$; il suo indice sarà al più il numero di elementi dell'insieme su cui agisce, quindi $l(\mathbf{C})$. La tesi discende allora dalla definizione di $\mathbb{Q}_{\mathbf{C}}$. □

Ora è semplice dare un primo criterio di rigidità.

Proposizione 2.17. *Nell'ipotesi che* S *sia fissato da* $\Gamma_{\mathbb{Q}}$ *il campo* $N_{\boldsymbol{\sigma}}$ *è di Galois su* $K_{\boldsymbol{\sigma}} := k_{\boldsymbol{\sigma}}(t)$*, e gli automorfismi di* $N_{\boldsymbol{\sigma}}/K_\sigma$ *agiscono su* $\mathrm{Gal}(N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t))$ *come automorfismi interni. Inoltre* $K_{\boldsymbol{\sigma}}$ *è il più piccolo campo che gode di questa proprietà.*

Dimostrazione. Sia $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}(t)/K_{\boldsymbol{\sigma}})$ e sia $\tilde{\delta}$ una sua estensione a N_S. Per definizione di $K_{\boldsymbol{\sigma}}$ vale $[\boldsymbol{\sigma}] = [\boldsymbol{\sigma}]^{\delta}$, per cui con la notazione scelta

$$\ker(\boldsymbol{\sigma})^{\tilde{\delta}} = \ker(\boldsymbol{\sigma}^{\tilde{\delta}^{-1}}) = \ker(\boldsymbol{\sigma}).$$

Tutte le estensioni lasciano invariato $N_{\boldsymbol{\sigma}}$, che quindi è di Galois su $K_{\boldsymbol{\sigma}}$. Ora sia $\tau \in G$ tale che $\boldsymbol{\sigma}^{\tilde{\delta}} = \boldsymbol{\sigma}^{\tau}$ (esiste per definizione di K_σ) e applichiamolo al sistema di generatori in $\mathrm{Gal}(N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t))$:

$$\varphi_{\boldsymbol{\sigma}}(\boldsymbol{\sigma})^{\tilde{\delta}} = \psi_{\boldsymbol{\sigma}}^{-1}(\boldsymbol{\sigma})^{\tilde{\delta}} \ker(\boldsymbol{\sigma}) = \psi_{\boldsymbol{\sigma}}^{-1}(\boldsymbol{\sigma}^{\tilde{\delta}}) \ker(\boldsymbol{\sigma}) = \varphi_{\boldsymbol{\sigma}}(\boldsymbol{\sigma}^{\tau}) = \varphi_{\boldsymbol{\sigma}}(\boldsymbol{\sigma})^{\varphi_\sigma(\tau)}.$$

$\tilde{\delta}$ agisce allora come automorfismo interno su un sistema di generatori, quindi su tutto G.

Viceversa se $N_{\boldsymbol{\sigma}}$ è di Galois su un campo K e i suoi automorfismi agiscono come automorfismi interni su G abbiamo che $[\boldsymbol{\sigma}^{\tilde{\delta}}] = [\boldsymbol{\sigma}]$, pertanto il suo gruppo di Galois è contenuto in $\Gamma_{\boldsymbol{\sigma}}$ e vale l'inclusione di campi richiesta. □

Quest'ultima proposizione insieme al teorema 2.10 ci dà una prima discesa:

Teorema 2.18. *Sia G un gruppo in cui il centro ha un complementare e $\boldsymbol{\sigma}$ un sistema di s generatori di G. Allora il campo $K_{\boldsymbol{\sigma}}$ è un campo di definizione per $N_{\boldsymbol{\sigma}}/_G\overline{\mathbb{Q}}(t)$.*

Dimostrazione. Abbiamo appena visto che $N_{\boldsymbol{\sigma}}/K_{\boldsymbol{\sigma}}$ è di Galois e gli automorfismi agiscono come automorfismi interni su $\mathrm{Gal}(N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t))$. Sia ora $\mathfrak{P}$ un posto di $\mathbb{P}^1(K_{\boldsymbol{\sigma}}/k_{\boldsymbol{\sigma}})$ di grado uno non ramificato in $N_{\boldsymbol{\sigma}}/K_{\boldsymbol{\sigma}}$.

Il gruppo di inerzia su $\mathfrak{P}$ è banale in quanto non vi è ramificazione, quindi il suo normalizzatore è l'intero gruppo G che ha complementare per il centro. Possiamo allora applicare il teorema 2.10 e dedurre che $K_{\boldsymbol{\sigma}}$ è un campo di definizione per $N_{\boldsymbol{\sigma}}/_G\overline{\mathbb{Q}}(t)$. □

Ora è sufficiente applicare tutte le ultime conclusioni nel caso rigido e otteniamo automaticamente il seguente criterio:

Teorema 2.19 (Criterio debole di rigidità)**.** *Sia G un gruppo finito in cui il centro ha un complementare e $\mathbf{C} \in \mathrm{Cl}(G)^s$ un vettore rigido di classi di G. Allora per qualsiasi scelta di s posti $\mathfrak{P}_i$ di grado uno in $\mathbb{Q}_{\mathbf{C}}(t)$ esiste un'estensione di Galois $N/\mathbb{Q}_{\mathbf{C}}(t)$ non ramificata fuori da S con*

$$\mathrm{Gal}(N/\mathbb{Q}_{\mathbf{C}}(t)) \cong G$$

e per la quale i gruppi di inerzia sopra i $\mathfrak{P}_i$ sono generati elementi σ_i nelle rispettive classi C_i.

Se il vettore è anche razionale abbiamo $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}$.

2.4 Rigidità forte

Il criterio può essere notevolmente migliorato se facciamo una scelta più oculata dei punti di ramificazione; faremo agire il gruppo simmetrico sui vettori di classi $\mathbf{C}$ come $(C_1, \dots, C_s)^\omega = (C_{\omega(1)}, \dots, C_{\omega(s)})$ e vedremo come questo ci porterà a realizzazioni su $\mathbb{Q}(t)$ con vettori non razionali. Diamo delle nuove definizioni:

Definizione 2.20. Chiamiamo *gruppo completo di simmetria di* $\mathbf{C}$ il gruppo

$$\mathrm{Sym}(\mathbf{C}) := \{\omega \in S_s \mid \mathbf{C}^\omega \in \mathbf{C}^*\}.$$

Un suo sottogruppo sarà chiamato *gruppo di simmetria di* $\mathbf{C}$.

Definizione 2.21. Sia V un gruppo di simmetria di $\mathbf{C}$. Definiamo

$$\mathbf{C}^V := \{\mathbf{C}^\omega \mid \omega \in V\}$$

e chiamiamo *grado di irrazionalità V-simmetrizzato di* $\mathbf{C}$ la quantità

$$d^V(\mathbf{C}) := |\mathbf{C}^*|/|\mathbf{C}^V|.$$

Un vettore per cui $d^V(\mathbf{C}) = 1$ è detto *V-simmetrico*.

Sulla falsariga delle definizioni precedenti scriviamo

$$\Gamma_{\mathbf{C}}^V := \{\delta \in \Gamma_{\mathbb{Q}} \mid \mathbf{C}^{c(\delta)} \in \mathbf{C}^V\}$$

e

$$\mathbb{Q}_{\mathbf{C}}^V := \overline{\mathbb{Q}}^{\Gamma_{\mathbf{C}}^V}.$$

Il primo risultato immediato è:

Proposizione 2.22. *Il campo* $\mathbb{Q}_{\mathbf{C}}^V$ *è un'estensione abeliana di* $\mathbb{Q}$ *contenuta in* $\mathbb{Q}_{\mathbf{C}}$ *di grado* $d^V(\mathbf{C})$.

Dimostrazione. Analogamente al caso debole l'azione di $\Gamma_{\mathbb{Q}}$ si fattorizza attraverso il carattere ciclotomico, pertanto l'estensione risultante è sicuramente abeliana.

Osserviamo ora che $\Gamma_{\mathbb{Q}}$ agisce transitivamente su $\mathbf{C}^*/\mathbf{C}^V$, quindi lo stabilizzatore di un qualsiasi elemento ha indice uguale a $d^V(\mathbf{C})$; per definizione però lo stabilizzatore della classe di $\mathbf{C}$ è proprio $\Gamma_{\mathbf{C}}^V$. □

Supponiamo ora che il luogo di ramificazione S sia solamente invariante per azione di $\Gamma_{\mathbb{Q}}$ ma in generale non fissato. Chiamiamo π_S la rappresentazione di permutazione di $\Gamma_{\mathbb{Q}}$ in S_s indotta dalla permutazione degli elementi di S; abbiamo che $\mathbf{C}^\delta \in \mathbf{C}^*$ se e soltanto se $\pi_S(\delta) \in \mathrm{Sym}(\mathbf{C})$.

Teorema 2.23. *Sia G un gruppo finito e* $\boldsymbol{\sigma} \in \Sigma(\mathbf{C})$, *con* $\mathbf{C} \in \mathrm{Cl}(G)^s$. *Sia S un insieme di s posti invariante per* $\Gamma_{\mathbb{Q}}$ *e* π_S *la rappresentazione di permutazione di* $\Gamma_{\mathbb{Q}}$ *associata. Se* $V = \pi_s(\Gamma_{\mathbb{Q}})$ *è un gruppo di simmetria di* $\mathbf{C}$ *allora il campo* K_σ *contiene* $\mathbb{Q}_{\mathbf{C}}^V$.

Se inoltre $\Gamma_{\mathbf{C}}^V$ *agisce come permutazione inversamente al carattere ciclotomico su* $\mathbf{C}^V$, *ovvero se* $\mathbf{C}^{\pi_S(\delta)} = \mathbf{C}^{c(\delta)^{-1}}$, *allora*

$$[K_{\boldsymbol{\sigma}} : \mathbb{Q}_{\mathbf{C}}^V(t)] \leq l(\mathbf{C}). \tag{2.4.1}$$

Dimostrazione. Per ogni $\delta \in \Gamma_{\boldsymbol{\sigma}}$ abbiamo $C_i^\delta = C_{i^\delta}^{c(\delta)} = C_i$ per il teorema 2.12, quindi $(\mathbf{C}^{\pi_S(\delta)})^{c(\delta)}$. Per ipotesi $\mathbf{C}^{\pi_S(\delta)} \in \mathbf{C}^V$, pertanto abbiamo $\mathbf{C}^{c(\delta)} \in \mathbf{C}^V$ e ne consegue $\delta \in \Gamma_{\mathbf{C}}^V$, così da avere l'inclusione richiesta.

Viceversa, se vale anche $\mathbf{C}^{\pi(\delta)} = \mathbf{C}^{c(\delta)^{-1}}$ otteniamo $\mathbf{C}^\delta = \mathbf{C}$ per tutti i $\delta \in \Gamma_{\mathbf{C}}^V$. Di conseguenza l'indice di $\Gamma_{\boldsymbol{\sigma}}$ in $\Gamma_{\mathbf{C}}^V$ è limitato dall'insieme delle possibili orbite, ovvero $l(\mathbf{C})$. □

Possiamo infine ottenere un rafforzamento del criterio di rigidità.

Teorema 2.24 (Criterio di rigidità forte)**.** *Sia G un gruppo finito il cui centro possiede un complementare e $\mathbf{C} \in \mathrm{Cl}(G)^s$ un vettore rigido di classi. Sia V un gruppo di simmetria di $\mathbb{C}$ tale che per ogni $\delta \in \Gamma_{\mathbf{C}}^V$ esiste un unico $\omega \in V$ per cui $\mathbf{C}^{c(\delta)} = \mathbf{C}^{\omega}$. Allora esiste un'estensione normale regolare $N/\mathbb{Q}_{\mathbf{C}}^V(t)$ con gruppo di Galois G.*

Se $\mathbf{C}$ è anche V-simmetrico allora $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$.

Dimostrazione. Decomponiamo l'insieme delle classi $\{C_1, \dots, C_s\}$ in orbite per l'azione di V. Per ogni orbita $\mathbf{B}$ costruiamo il relativo gruppo

$$\Gamma_{\mathbf{B}} = \{\delta \in \Gamma_{\mathbf{C}}^V \mid C_i^{c(\delta)} = C_i \ \forall C_i \in \mathbf{B}\}.$$

Questo gruppo contiene $\Gamma_{\mathbf{C}}$ mentre $\Gamma_{\mathbf{C}}^V/\Gamma_{\mathbf{B}}$ agisce fedelmente e transitivamente su $\mathbf{B}$; pertanto $\mathbb{Q}_{\mathbf{B}} = \overline{\mathbb{Q}}^{\Gamma_{\mathbf{B}}}$ è contenuto in $\mathbb{Q}_{\mathbf{C}}$ e contiene $\mathbb{Q}_{\mathbf{C}}^V$, sul quale ha grado $|\mathbf{B}|$.

Scegliamo ora una classe C_i qualsiasi di $\mathbf{B}$ e gli associamo un elemento primitivo a_i di $\mathbb{Q}_{\mathbf{B}}/\mathbb{Q}_{\mathbf{C}}^V$. Al variare di $\overline{\delta} \in \Gamma_{\mathbf{C}}^V/\Gamma_{\mathbf{B}}$ definiamo $\mathfrak{P}_{\omega(i)} = (t - a_i^{\overline{\delta}^{-1}})$, dove ω è usa permutazione associata a δ, in modo da assegnare ad ogni classe di $\mathbf{B}$ un posto $\mathfrak{P}_j$ (la definizione è buona poiché le permutazioni ω possibili coincidono per costruzione su $\mathbf{B}$).

A meno di adattare la scelta degli a_i possiamo fare in modo che tutti i $\mathfrak{P}_j$ siano distinti e formino un insieme S di s elementi invariante per $\Gamma_{\mathbb{Q}}$. Per costruzione abbiamo che $\pi_S(\delta) = \omega^{-1}$, per cui

$$\mathbf{C}^{\delta} = (\mathbf{C}^{\omega^{-1}})^{c(\delta)} = \mathbf{C}.$$

Quindi ora possiamo applicare il teorema precedente ed ottenere l'estensione richiesta. □

La richiesta su V, necessaria per costruire l'insieme S in modo che $\pi_S(\delta)$ sia la permutazione corrispondente alla permutazione delle classi di coniugio determinata dall'esponenziazione per $c(\delta)$. Definiamo

$$\mathrm{Inv}(\mathbf{C}) = \{\omega \mid \omega(\mathbf{C}) = \mathbf{C}\} \subset \mathrm{Sym}(\mathbf{C})$$

come il gruppo delle permutazioni che lasciano invariato il vettore $\mathbf{C}$. Tale gruppo è ovviamente banale se le classi di coniugio sono tutte distinte. La richiesta del teorema 2.24 è soddisfatta allora esattamente quando $V \cap \mathrm{Inv}(\mathbf{C}) = \{e\}$, poiché allora la permutazione indotta da $c(\delta)$ per qualche $\delta \in \Gamma_{\mathbb{C}}^V$ identifica un unico elemento di V.

Per la proposizione 2.17 e il teorema 2.23 il criterio di rigidità forte non può essere migliorato se non sulla costante $l(\mathbf{C})$; infatti data una qualsiasi G-realizzazione regolare di G su un campo $k(t)$, con k estensione finita di $\mathbb{Q}$, essa si immergerà in un'opportuna estensione N_S di $\overline{\mathbb{Q}}(t)$, verranno identificati dei generatori con le rispettive classi di coniugio e allora sarà identificato un campo minimale $k_{min} \subset k$. Con tecniche più generali è però possibile ottenere, in alcuni casi speciali, maggiorazioni migliori della (2.4.1).

2.5 Automorfismi geometrici

Si può estendere la ricerca dei campi di definizione sfruttando il gruppo $\mathrm{Aut}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}})$; ogni sottocampo di $\overline{\mathbb{Q}}(t)$ contenente $\overline{\mathbb{Q}}$ è infatti, per il teorema di Lüroth, della forma $\overline{\mathbb{Q}}(\tilde{t})$, dandoci quindi delle informazioni aggiuntive sui campi realizzabili geometricamente su $\overline{\mathbb{Q}}$. Studiamo innanzitutto il gruppo $\mathrm{Aut}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}) \cong \mathrm{PGL}_2(\overline{\mathbb{Q}})$.

Teorema 2.25. *Sia J un sottogruppo di $\mathrm{Aut}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}})$. Allora J è isomorfo a Z_n, D_n, A_4, S_4 oppure A_5. Inoltre vi sono solo 3 posti ramificati in $\mathbb{P}(\overline{\mathbb{Q}}(t)^J/\overline{\mathbb{Q}})$ e i tre posti insieme ai rispettivi indici di ramificazione identificano univocamente l'estensione $\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(t)^J$.*

Dimostrazione. Supponiamo che vi siano s posti di $\mathbb{P}(\overline{\mathbb{Q}}(t)^J/\overline{\mathbb{Q}})$ ramificati in $\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(t)^J$ (chiaramente $s \geq 2$); l'estensione è normale, quindi ognuno di essi ha un unico indice di ramificazione che chiameremo e_i. Scriviamo la formula di Hurwitz:

$$\begin{aligned}
(2g(\overline{\mathbb{Q}}(t)^J/\overline{\mathbb{Q}}) - 2) &= (2g(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}) - 2)|J| + \sum_{i=1}^{s} \frac{|J|}{e_i}(e_i - 1) \\
-2 &= -2|J| + |J| \sum_{i=1}^{s} \left(1 - \frac{1}{e_i}\right) \\
2\left(1 - \frac{1}{|J|}\right) &= s - \sum_{i=1}^{s} \frac{1}{e_i}.
\end{aligned}$$

Riordiniamo gli e_i in modo che sia $1 < e_1 \leq \ldots \leq e_s$; dato che in particolare $e_i \geq 2$, $s - \sum_i 1/e_i \geq s/2$ e quindi $s \leq 3$. Nel caso $s = 2$ poniamo $e_1 = e_1' d$ e $e_2 = e_2' d$ con $(e_1', e_2') = 1$:

$$\begin{aligned}
2\left(1 - \frac{1}{|J|}\right) &= 2 - \frac{e_1 + e_2}{e_1 e_2} \\
\frac{2}{|J|} &= \frac{e_1' + e_2'}{e_1' e_2' d}
\end{aligned}$$

di conseguenza $e_1' = e_2' = 1$ e $d = |J|$. Nel caso $s = 3$ abbiamo invece:

$$1 + \frac{2}{|J|} = \frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3}.$$

Se tutti gli indici fossero maggiori di 2 il membro a destra varrebbe 1; vale pertanto $e_1 = 2$. Se poniamo $e_2 = 2$ abbiamo $e_3 = |J|/2$. Se invece i restanti indici fossero maggiori di 3 il membro a destra varrebbe 1, quindi rimane il caso $e_2 = 3$. I valori possibili rimanenti per e_3 sono infine 3, 4 e 5, ed in tutti i casi esiste un valore intero di $|J|$ opportuno.

Per la classificazione di Hurwitz possiamo trovare al più gruppi della forma

$$J = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \quad \sigma_1^{e_1} = \sigma_2^{e_2} = \sigma_3^{e_3} = e \quad \sigma_1\sigma_2\sigma_3 = e \quad |J| = n_{e_1,e_2,e_3}$$

dove n_{e_1,e_2,e_3} è il valore di $|J|$ che risolve le equazioni precedenti, o della forma

$$J = \langle \sigma_1, \sigma_2 \rangle \quad \sigma_1^{e_1} = \sigma_2^{e_2} = e \quad \sigma_1\sigma_2 = e \quad |J| = e_1.$$

Nel secondo caso il gruppo esiste ed è evidentemente Z_n. Nel primo caso si calcola facilmente che le relazioni richieste forniscono esattamente le presentazioni di D_n, A_4, S_5, A_5.

Conseguenza di ciò è che ogni altra scelta di tre generatori soddisfacente le relazioni date è coniugata tramite $\mathrm{Aut}(J)$, quindi la classificazione di Hurwitz ci dice che fissati tre punti di ramificazione in $\overline{\mathbb{Q}}(t)$ esiste un'unica estensione con gruppo J e indici di ramificazione assegnati. □

Fissiamo ora la notazione per poter parlare degli automorfismi geometrici in termini analoghi a quelli usati nelle sezioni precedenti. Chiamiamo A_S il gruppo di automorfismi che lascia fisso il luogo di ramificazione S

$$A_S := \{\eta \in \mathrm{Aut}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}) \mid S^\eta = S\}.$$

Sia $\pi_S : A_S \to S_s$ la rappresentazione di permutazione associata. Per ogni sottogruppo V di $\pi_S(A_S)$ chiamiamo

$$A_S^V := \pi_S^{-1}(V) = \{\eta \in A_S \mid \pi_S(\eta) \in V\}. \tag{2.5.7}$$

Proposizione 2.26. *Per $s \geq 3$ la rappresentazione π_S è fedele. In particolare per ogni $V \in \pi_S(A_S)$*

$$A_S^V \cong V.$$

Dimostrazione. Ogni elemento $\varphi \in \mathrm{Aut}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}})$ è della forma:

$$\varphi(t) = \frac{at + c}{bt + d}$$

con $ad - bc \neq 0$. L'azione corrispondente sui posti, letta in termini di punti di $\mathbb{P}^1(\overline{\mathbb{Q}})$, è data da

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

pertanto è determinata dall'azione su tre punti qualsiasi distinti. La rappresentazione è quindi fedele. □

Gli automorfismi $\eta \in A_S$, per definizione, lasciano invariato S, pertanto qualunque estensione alla chiusura algebrica $\overline{\overline{\mathbb{Q}}(t)}$ lascia invariato N_S; in particolare quindi ogni η si estende ad un automorfismo di $N_S/\overline{\mathbb{Q}}$. Due estensioni $\tilde{\eta}$ e $\tilde{\eta}'$ sono tali che $\tilde{\eta}^{-1} \circ \tilde{\eta}' \in \Gamma_s$; quindi se analogamente alla (2.3.2) costruiamo un'azione a destra su $\Sigma_s(G)$ dall'insieme $\tilde{A}_S$ delle possibili estensioni di A_S

$$\begin{aligned} \Sigma_s(G) \times \tilde{A}_S \quad &\to \quad \Sigma_s(G) \\ (\boldsymbol{\sigma}, \tilde{\eta}) \to \boldsymbol{\sigma}.\tilde{\eta} = \boldsymbol{\sigma}^{\tilde{\eta}^{-1}} \quad &\text{con } \boldsymbol{\sigma}^{\tilde{\eta}} = \psi_{\boldsymbol{\sigma}}(\gamma^{\tilde{\eta}}). \end{aligned}$$

l'azione su $\Sigma_s(G)/\mathrm{Inn}(G)$ non dipenderà dall'estensione scelta e sarà quindi un'azione da A_S.

Definiamo il nuovo insieme

$$\Sigma(\mathbf{C}^V) := \bigcup_{\omega \in V} \Sigma(\mathbf{C}^\omega).$$

L'azione di A_S^V si trasferisce quindi su $\Sigma(\mathbf{C}^V)/\operatorname{Inn}(G)$. Il numero di orbite di questa azione verrà denotato con $l^V(\mathbf{C})$. Diamo un nome allo stabilizzatore di un elemento

$$A_{\boldsymbol{\sigma}}^V := \{\eta \in A_S^V \mid [\boldsymbol{\sigma}]^\eta = [\boldsymbol{\sigma}]\}$$

e definiamo un indice di rigidità "parziale"

$$l_U^V(\mathbf{C}) := |\{[\boldsymbol{\sigma}]^{A_S^V} \mid \boldsymbol{\sigma} \in \Sigma(\mathbf{C}), A_{\boldsymbol{\sigma}}^V = U^\alpha \text{ per un } \alpha \in \operatorname{Aut}(A_S^V)\}|$$

contando le orbite il cui stabilizzatore è U a meno di automorfismo.

Definizione 2.27. Se un'orbita dell'azione di A_S^V su $\Sigma(\mathbf{C}^V)/\operatorname{Inn}(G)$ è tale che $l_{H_{\boldsymbol{\sigma}}^V}^V(\mathbf{C}) = 1$, allora tale orbita viene detta *A_S^V-orbita rigida*.

Se inoltre $\Sigma(\mathbf{C}^V)/\operatorname{Inn}(G)$ è una sola A_S^V-orbita (rigida) allora $\mathbf{C}$ viene detto *vettore di classi V-rigido*.

Estendiamo ora il gruppo $\Gamma_{\mathbb{Q}}$ in modo da includere gli automorfismi geometrici

$$\Gamma_S^V := \langle \Gamma_{\mathbb{Q}}, A_S^V \rangle < \operatorname{Aut}(\overline{\mathbb{Q}}(t)/\mathbb{Q}) \tag{2.5.10}$$

e definiamo il nuovo stabilizzatore degli elementi di $\Sigma_s(G)/\operatorname{Inn}(G)$

$$\Gamma_{\boldsymbol{\sigma}}^V := \{\delta \in \Gamma_S^V \mid [\boldsymbol{\sigma}]^\delta = [\boldsymbol{\sigma}]\}.$$

Osservazione 2.28. Il carattere ciclotomico si estende su $\Gamma_{\boldsymbol{\sigma}}^V$ in modo naturale, poiché A_S^V agisce banalmente su $\overline{\mathbb{Q}}$, in particolare sulle radici dell'unità. Il suo kernel conterrà quindi A_S^V.

Definizione 2.29. Un insieme s posti $S \subset \mathbb{P}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}})$ viene detto *V-configurazione*, con $V < S_s$, se $\pi_S(\Gamma) \subset V$ e se inoltre $A_S^V \cong V$.

Possiamo allora generalizzare il teorema 2.23

Teorema 2.30. *Sia G un gruppo finito e $\boldsymbol{\sigma} \in \Sigma(\mathbf{C})$, con $\mathbf{C} \in \mathrm{Cl}(G)^s$, V un gruppo di simmetria di $\mathbf{C}$ e S un insieme di s posti che sia una V-configurazione.*

Se chiamiamo $K_{\boldsymbol{\sigma}}^V$ il campo fisso di $\Gamma_{\boldsymbol{\sigma}}^V$ e $k_{\boldsymbol{\sigma}}^V$ la chiusura algebrica di $\mathbb{Q}$ in $K_{\boldsymbol{\sigma}}^V$ abbiamo la relazione

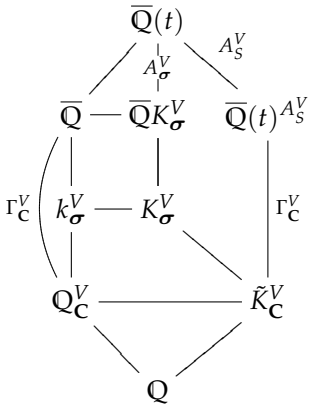
$$[k_{\boldsymbol{\sigma}}^V : \mathbb{Q}_{\mathbf{C}}^V] \leq l_{A_{\boldsymbol{\sigma}}^V}^V(\mathbf{C}).$$

In particolare l'estensione $K_{\boldsymbol{\sigma}}^V/\mathbb{Q}_{\mathbf{C}}^V$ è regolare se $[\boldsymbol{\sigma}]^{A_S^V}$ è un'orbita rigida.

Dimostrazione. Notiamo che per ogni elemento $\delta \in \Gamma_{\boldsymbol{\sigma}}^V$ vale $\pi_S(\delta) \in V$ per l'ipotesi fatta su S, quindi da $\mathbf{C}^\delta = \mathbf{C}$ ricaviamo $\mathbf{C}^{c(\delta)} = \mathbf{C}^{\pi_S(\delta)^{-1}} \in \mathbf{C}^V$; in particolare allora esso apparterrà al gruppo $\tilde{\Gamma}_{\mathbf{C}}^V := \langle \Gamma_{\mathbf{C}}^V, A_S^V \rangle$.

Il gruppo $\tilde{\Gamma}_{\mathbf{C}}^V$ agisce su $\Sigma(\mathbf{C}^V)/\operatorname{Inn}(G)$; poiché A_S^V è un sottogruppo normale di Γ_S^V abbiamo che $A_{\boldsymbol{\sigma}^\delta}^V = (A_{\boldsymbol{\sigma}}^V)^{\delta^{-1}}$, dove δ agisce come automorfismo di A_S^V. Ponendo $\tilde{K}_{\mathbf{C}}^V := \overline{\mathbb{Q}}(t)^{\tilde{\Gamma}_{\mathbf{C}}^V}$ vale allora la diseguaglianza

$$[K_{\boldsymbol{\sigma}}^V : \tilde{K}_{\mathbf{C}}^V] = (\tilde{\Gamma}_{\mathbf{C}}^V : \Gamma_{\boldsymbol{\sigma}}^V) \leq (A_S^V : A_{\boldsymbol{\sigma}}^V) l_{A_{\boldsymbol{\sigma}}^V}^V(\mathbf{C}).$$



Per costruzione l'estensione $\tilde{K}_{\mathbf{C}}^V/\mathbb{Q}_{\mathbf{C}}^V$ è regolare, mentre vale $\overline{\mathbb{Q}}K_{\boldsymbol{\sigma}}^V = \overline{\mathbb{Q}}(t)^{A_{\boldsymbol{\sigma}}^V}$, quindi

$$[k_{\boldsymbol{\sigma}}^V : \mathbb{Q}_{\mathbf{C}}^V] = \frac{[K_{\boldsymbol{\sigma}}^V : \tilde{K}_{\mathbf{C}}^V]}{[\overline{\mathbb{Q}}K_{\boldsymbol{\sigma}}^V : \overline{\mathbb{Q}}\tilde{K}_{\mathbf{C}}^V]} = \frac{(\tilde{\Gamma}_{\mathbf{C}}^V : \Gamma_{\boldsymbol{\sigma}}^V)}{(A_S^V : A_{\boldsymbol{\sigma}}^V)} \leq l_{A_{\boldsymbol{\sigma}}^V}^V(\mathbf{C}).$$

In particolare l'estensione $K_{\boldsymbol{\sigma}}^V/\mathbb{Q}_{\mathbf{C}}^V$ è regolare se $[\boldsymbol{\sigma}]^{A_S^V}$ è un'orbita rigida. □

Il teorema appena enunciato non basta, però, a dare realizzazioni su $\mathbb{Q}_{\mathbf{C}}^V$, poiché non è detto che l'estensione $K_{\boldsymbol{\sigma}}^V/k_{\boldsymbol{\sigma}}^V$ sia razionale.

Teorema 2.31. *Ogni sottocampo K di $\overline{\mathbb{Q}}(t)$ trascendente su $\mathbb{Q}$ ha genere 0 come campo di funzioni su $\overline{\mathbb{Q}} \cap K$.*

Dimostrazione. Si veda [1, Th. 16.7]. □

Teorema 2.32. *Un campo di funzioni K/k di genere 0 è razionale se e soltanto se ha un posto di grado dispari.*

Dimostrazione. Fissiamo la notazione: $\mathfrak{P}$ sarà un posto generico di $\mathbb{P}(K/k)$, con valutazione associata $v_{\mathfrak{P}}$ e grado $f(\mathfrak{P})$, $\mathcal{L}(\mathfrak{a})$ lo spazio degli elementi di K con divisore multiplo di $-\mathfrak{a}$, $l(\mathfrak{a})$ la dimensione di $\mathcal{L}(\mathfrak{a})$ come spazio vettoriale su k, $d(\mathfrak{a})$ il grado di $\mathfrak{a}$, $\operatorname{div}(x)$ il divisore di $x \in K$, $\operatorname{div}_\infty(x)$ il divisore dei poli e infine $\mathfrak{d}$ un divisore della classe canonica.

Richiamiamo la formula di Riemann-Roch:

$$l(\mathfrak{a}) = d(\mathfrak{a}) + l(\mathfrak{d} - \mathfrak{a}) + 1 - g. \tag{2.5.11}$$

Ricordiamo inoltre che $d(\mathfrak{a}) = 2g - 2$ e se $d(\mathfrak{a}) > 2g - 2$ vale $l(\mathfrak{d} - \mathfrak{a}) = 0$. Supponiamo allora che sia $g = 0$ e che esista un posto $\mathfrak{P}$ di grado dispari. Poniamo $\mathfrak{a} := \mathfrak{P} - k\mathfrak{d}$ in modo che sia $d(\mathfrak{a}) = 1 > -2$. Otteniamo, applicando la formula (2.5.11),

$$l(\mathfrak{a}) = d(\mathfrak{a}) + l(\mathfrak{d} - \mathfrak{a}) + 1 = 2.$$

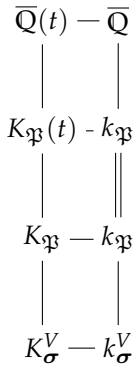
Troviamo quindi due elementi $\alpha, \beta \in \mathcal{L}(\mathfrak{a})$ linearmente indipendenti; ponendo $x := \beta/\alpha$ abbiamo che 1 e x appartengono a $\mathcal{L}(\operatorname{div}(\alpha) + \mathfrak{a})$. In particolare $\mathfrak{P}' := \operatorname{div}(\alpha) + \mathfrak{a}$ è un divisore intero e il suo grado è $d(\mathfrak{P}') = d(\mathfrak{a}) = 1$, quindi è in realtà un posto di grado 1. Inoltre $\operatorname{div}(x) + \mathfrak{P}'$ è un divisore intero, quindi otteniamo che

$$[K : k(x)] = d(\operatorname{div}_\infty(x)) = d(\mathfrak{P}') = 1.$$

Se viceversa $K = k(x)$, allora $d(\mathrm{div}_\infty(x))$ è un posto di grado 1, e in particolare ha grado dispari. □

Proposizione 2.33. *Nelle ipotesi del teorema 2.30 se V possiede un'orbita di lunghezza dispari in $\{1,\dots,s\}$ il campo $K_{\boldsymbol{\sigma}}^V$ è razionale su $k_{\boldsymbol{\sigma}}^V$.*

Dimostrazione. Sia $\mathfrak{P}$ un posto di $\mathbb{P}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}})$ tale che la sua orbita per V sia di ordine dispari; sia $\Gamma_{\mathfrak{P}}$ il suo stabilizzatore per l'azione di $\Gamma_{\boldsymbol{\sigma}}^V$. Poiché quest'ultimo gruppo agisce come sottogruppo di V, l'orbita di $\mathfrak{P}$ sarà di ordine dispari anche per la sua azione, quindi in particolare $(\Gamma_{\boldsymbol{\sigma}}^V : \Gamma_{\mathfrak{P}})$ è dispari.



Siano ora $K_{\mathfrak{P}} := \overline{\mathbb{Q}}(t)^{\Gamma_{\mathfrak{P}}}$, $k_{\mathfrak{P}} := K_{\mathfrak{P}} \cap \overline{\mathbb{Q}}$ e $\mathfrak{P}' := \mathfrak{P}|_{K_{\mathfrak{P}}} \in \mathbb{P}(K_{\mathfrak{P}}|k_{\mathfrak{P}})$. Se $(t-\alpha)$ è un parametro locale di $\mathfrak{P}$, con $\alpha \in \overline{\mathbb{Q}}$, dobbiamo avere $\alpha \in k_{\mathfrak{P}}(t) = K_{\mathfrak{P}}(t)$, poiché il gruppo di Galois associato a $K_{\mathfrak{P}}(t)$ lascia fisso sia t che $\mathfrak{P}$, quindi anche α. Il campo residuo di $\mathfrak{P}|k_{\mathfrak{P}}(t)$ è quindi $k_{\mathfrak{P}}$, ma essendo tale posto anche un'estensione di $\mathfrak{P}'$, anche $\mathfrak{P}'$ ha campo residuo $k_{\mathfrak{P}}$, quindi è di grado 1. Dato ora che $\mathfrak{P}'$ è un'estensione di $\mathfrak{P}'' := \mathfrak{P}'|_{K_{\boldsymbol{\sigma}}^V}$, il campo residuo di $\mathfrak{P}''$ è una sottoestensione di $k_{\mathfrak{P}}/k_{\boldsymbol{\sigma}}^V$; il grado di quest'ultima estensione è un divisore di $[K_{\mathfrak{P}} : K_{\boldsymbol{\sigma}}^V] = (\Gamma_{\boldsymbol{\sigma}}^V : \Gamma_{\mathfrak{P}})$, quindi è dispari, quindi anche il campo residuo di $\mathfrak{P}''$ ha grado dispari su $k_{\boldsymbol{\sigma}}^V$. Per definizione quindi $\mathfrak{P}''$ è un posto di grado dispari.

Ora per il teorema 2.31 $K_{\boldsymbol{\sigma}}^V$ ha genere 0; per quanto detto appena detto ha un posto di grado dispari, quindi è razionale per il teorema 2.32. □

Possiamo quindi enunciare il criterio finale.

Teorema 2.34 (Criterio di rigidità torta)**.** *Sia G un gruppo finito il cui centro possiede un complementare e $\mathbf{C} \in \mathrm{Cl}(G)^s$ un vettore di classi. Sia V un gruppo di simmetria di $\mathbb{C}$ con un'orbita di lunghezza dispari in $\{1,\dots,s\}$ e una V-configurazione S. Se $\Sigma(\mathbf{C}^V)/\mathrm{Inn}(G)$ contiene un'orbita A_S^V-rigida esiste un'estensione normale regolare $N/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ con gruppo di Galois G.*

Se $\mathbf{C}$ è anche V-simmetrico allora $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$.

2.6 Gruppi di automorfismi

Il criterio di rigidità può essere esteso se al posto di realizzare G cerchiamo di ottenere la realizzazione di un gruppo H, con $\mathrm{Inn}(G) < H < \mathrm{Aut}(G)$. Quando il centro di G è banale otterremo quindi anche delle realizzazioni di G sotto opportune ipotesi aggiuntive.

Fissiamo della nuova notazione estendendo le vecchie definizioni:

$$\mathbf{C}^H := \{\mathbf{C}^\alpha \mid \alpha \in H\}$$
$$\mathrm{Sym}(\mathbf{C}^H) := \{\omega \in S_s \mid \mathbf{C}^{\omega\alpha} \in \mathbf{C}^H \text{ per qualche } \alpha \in H\}$$

e chiamiamo *gruppi di simmetria di* $\mathbf{C}^H$ i sottogruppi $V < \mathrm{Sym}(\mathbf{C}^H)$. Manteniamo quindi le stesse definizioni dei gruppi A_S^V e Γ_S^V date in (2.5.7) e (2.5.10). Al

variare di $\boldsymbol{\sigma}^H \in \Sigma(\mathbf{C}^H)/H$ definiamo stabilizzatori e campi fissi:

$$\Gamma^V_{\boldsymbol{\sigma}^H} := \{\delta \in \Gamma^V_S \mid \boldsymbol{\sigma}^{\delta H} = \boldsymbol{\sigma}^H\}, \quad K^V_{\boldsymbol{\sigma}^H} := \overline{\mathbb{Q}}(t)^{\Gamma^V_{\boldsymbol{\sigma}^H}}$$
$$H^V_{\boldsymbol{\sigma}^H} := A^V_S \cap \Gamma_{\boldsymbol{\sigma}^H{}^V}, \quad K'_{\boldsymbol{\sigma}^H{}^V} := \overline{\mathbb{Q}}(t)^{\Gamma^V_{\boldsymbol{\sigma}^H}}.$$

Proposizione 2.35. *Se il campo $K^V_{\boldsymbol{\sigma}^H}$ è dischiuso, allora è un campo di definizione per $N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t)$.*

Dimostrazione. Sia $\delta \in \Gamma^V_{\boldsymbol{\sigma}^H}$ un automorfismo di $\overline{\mathbb{Q}}(t)/K^V_{\boldsymbol{\sigma}^H}$. Per ipotesi ogni δ lascia invariante S, quindi si estende a $\tilde{\delta}$ su N_S. Ci basta allora scrivere l'azione di $\tilde{\delta}$ su $\ker(\boldsymbol{\sigma})$:

$$\ker(\boldsymbol{\sigma})^{\tilde{\delta}} = \ker(\boldsymbol{\sigma}^{\tilde{\delta}^{-1}}) = \ker(\boldsymbol{\sigma}^{\alpha}) = \ker(\boldsymbol{\sigma})$$

poiché la classificazione di Hurwitz è proprio a meno di automorfismi. In particolare allora $N_{\boldsymbol{\sigma}}/K^V_{\boldsymbol{\sigma}^H}$ è normale e per il teorema 2.7 è $K^V_{\boldsymbol{\sigma}^H}$ è di definizione per $N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t)$. □

Osservazione 2.36. Per un ragionamento identico a quello della proposizione 2.33, se V ha un'orbita di lunghezza dispari in S allora $K^V_{\boldsymbol{\sigma}^H}$ è dischiuso e razionale della forma $k^V_{\boldsymbol{\sigma}^H}(t)$, con $k^V_{\boldsymbol{\sigma}^H} \subset \overline{\mathbb{Q}}$.

Cerchiamo ora di stimare il grado di $k^V_{\boldsymbol{\sigma}^H}$ su $\mathbb{Q}$. Analogamente ai ragionamenti fatti finora definiamo

$$\mathbf{C}^{HV} := \{\mathbf{C}^{\alpha\omega} \mid \alpha \in H, \omega \in V\}$$

e ne prendiamo lo stabilizzatore in Γ tramite l'azione del carattere ciclotomico

$$\Gamma^{HV}_{\mathbf{C}} := \{\delta \in \Gamma \mid \mathbf{C}^{c(\delta)} \in \mathbf{C}^{HV}\}.$$

Definizione 2.37. Si dice *grado di irrazionalità HV-simmetrizzato di* $\mathbf{C}$ la quantità

$$d^{HV}(\mathbf{C}) := (\Gamma : \Gamma^{HV}_{\mathbf{C}}) = \frac{|\mathbf{C}^*|}{|\mathbf{C}^{HV} \cap \mathbf{C}^*|}.$$

Il vettore $\mathbf{C}$ si dice HV-simmetrico se $d^{HV}(\mathbf{C}) = 1$.

Confrontando gli indici otteniamo immediatamente

Proposizione 2.38. *Il campo fisso $\mathbb{Q}^{HV}_{\mathbf{C}} := \overline{\mathbb{Q}}^{\Gamma^{HV}_{\mathbf{C}}}$ è abeliano e contenuto in $\mathbb{Q}_{\mathbf{C}}$ con grado*

$$[\mathbb{Q}^{HV}_{\mathbf{C}} : \mathbb{Q}] = d^{HV}(\mathbf{C}).$$

In particolare $\mathbb{Q}^{HV}_{\mathbf{C}} = \mathbb{Q}$ se $\mathbf{C}$ è HV-simmetrico.

Definiamo di nuovo la quantità

$$l^V_U(\mathbf{C}) := |\{\boldsymbol{\sigma}^{HA^V_S} \mid \boldsymbol{\sigma} \in \Sigma(\mathbf{C}), A^V_{\boldsymbol{\sigma}} = U^{\alpha} \text{ per un } \alpha \in \mathrm{Aut}(A^V_S)\}|$$

per contare il numero di A_S^V-orbite in $\Sigma(\mathbf{C}^{HV})/H$ con stabilizzatore $U < A_S^V$ (a meno di automorfismo). Diciamo quindi anche che $\boldsymbol{\sigma}^{HA_S^V}$ è un'orbita A_S^V-rigida se $l_U^{HV}(\mathbf{C}) = 1$ per $U = A^V_{\boldsymbol{\sigma}^H}$. Se $\Sigma(\mathbf{C}^{HV})/H$ consiste di una sola A_S^V-orbita, il vettore $\mathbf{C}$ si dice HV-rigido.

Teorema 2.39. *Sia G un gruppo finito, $\mathrm{Inn}(G) < H < \mathrm{Aut}(G)$, $\mathbf{C} \in \mathrm{Cl}(G)^s$ con $s \geq 3$, V un gruppo di simmetria di $\mathbf{C}^H$ e S una V-configurazione. Allora il campo fisso $K^V_{\boldsymbol{\sigma}^H}$ contiene $\mathbb{Q}_{\mathbf{C}}^{HV}$. Per il grado di $k^V_{\boldsymbol{\sigma}^H} := K^V_{\boldsymbol{\sigma}^A} \cap \overline{\mathbb{Q}}$ vale*

$$[k^V_{\boldsymbol{\sigma}^H} : \mathbb{Q}_{\mathbf{C}}^{HV}] \leq l^{HV}_{A^V_{\boldsymbol{\sigma}^H}}(\mathbf{C}).$$

In particolare $K^V_{\boldsymbol{\sigma}^H}/\mathbb{Q}_{\mathbf{C}}^{HV}$ è regolare se $\boldsymbol{\sigma}^{HA_S^V}$ è un'orbita rigida.

Dimostrazione. La dimostrazione è identica a quella del teorema 2.30: dall'ipotesi $\pi_S(\Gamma) < V$ ricaviamo $\mathbf{C}^{c(\delta)} \in \mathbf{C}^{HV}$ per ogni $\delta \in \Gamma^V_{\boldsymbol{\sigma}^H}$, ossia, definendo $\tilde{\Gamma}_{\mathbf{C}}^{HV} := \langle \Gamma_{\mathbf{C}}^{HV}, A_S^V \rangle$, $\Gamma^V_{\boldsymbol{\sigma}^H} < \tilde{\Gamma}_{\mathbf{C}}^{HV}$. Otteniamo di nuovo $A^V_{\boldsymbol{\sigma}^{\delta H}} = (A^V_{\boldsymbol{\sigma}^H})^{\delta^{-1}}$ e chiamando $\tilde{K}_{\mathbf{C}}^{HV}$ il campo fisso di $\tilde{\Gamma}_{\mathbf{C}}^{HV}$

$$[K^V_{\boldsymbol{\sigma}^H} : \tilde{K}_{\mathbf{C}}^{HV}] = [\tilde{\Gamma}_{\mathbf{C}}^{HV} : \Gamma^V_{\boldsymbol{\sigma}^H}] < (A_S^V : A^V_{\boldsymbol{\sigma}^H}) \cdot l^{HV}_{A^V_{\boldsymbol{\sigma}^H}}(\mathbf{C}).$$

Quindi

$$[k^V_{\boldsymbol{\sigma}^H} : \mathbb{Q}_{\mathbf{C}}^{HV}] = \frac{[K^V_{\boldsymbol{\sigma}^H} : \tilde{K}_{\mathbf{C}}^{HV}]}{[\overline{\mathbb{Q}}K^V_{\boldsymbol{\sigma}^H} : \overline{\mathbb{Q}}\tilde{K}_{\mathbf{C}}^{HV}]} = \frac{(\tilde{\Gamma}_{\mathbf{C}}^{HV} : \Gamma^V_{\boldsymbol{\sigma}^H})}{(A_S^V : A^V_{\boldsymbol{\sigma}^H})} \leq l^{HV}_{A^V_{\boldsymbol{\sigma}^H}}(\mathbf{C}).$$

Se $\boldsymbol{\sigma}^{HA_S^V}$ è rigido si ottiene immediatamente la regolarità di $K^V_{\boldsymbol{\sigma}^H}/\mathbb{Q}_{\mathbf{C}}^{HV}$. □

Proposizione 2.40. *Siano G, H e $\mathbf{C}$ come nel teorema 2.39, V un gruppo di simmetria di $\mathbf{C}^H$ e $\boldsymbol{\sigma} \in \Sigma(\mathbf{C}^H)$ tale per cui $\boldsymbol{\sigma}^H \subset [\boldsymbol{\sigma}]^{\Gamma_S^V}$. Esiste allora un'estensione di Galois $N^H/K^V_{\boldsymbol{\sigma}^H}$ con*

$$\mathrm{Gal}(N^H/K^V_{\boldsymbol{\sigma}^H}) \cong A, \quad \mathrm{Gal}(N^H/K^V_{\boldsymbol{\sigma}}) \cong \mathrm{Inn}(G).$$

$N^H/K^v_{\boldsymbol{\sigma}}$ è regolare.

Dimostrazione. Nella proposizione 2.35 abbiamo visto che l'estensione $N_{\boldsymbol{\sigma}}/K^V_{\boldsymbol{\sigma}^H}$ è di Galois. Sia allora N^H il campo fisso del centralizzatore del suo gruppo di Galois e $N^H_{\boldsymbol{\sigma}}$ il campo fisso del centralizzatore di $\mathrm{Gal}(N_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t))$. Vale ovviamente $\overline{\mathbb{Q}}(t)N^H = N^H_{\boldsymbol{\sigma}}$. Il gruppo generato da G e dal centralizzatore è invece $\Gamma^V_{\boldsymbol{\sigma}}$, quindi

$$\mathrm{Gal}(N^H/K^V_{\boldsymbol{\sigma}}) \cong \mathrm{Gal}(N^H_{\boldsymbol{\sigma}}/\overline{\mathbb{Q}}(t)) \cong \mathrm{Inn}(G).$$

L'estensione $N^H/K^V_{\boldsymbol{\sigma}}$ è quindi regolare. Inoltre $\mathrm{Gal}(N^H/K^V_{\boldsymbol{\sigma}^H})$ è isomorfo ad un sottogruppo di H. L'ipotesi che H agisca sull'orbita di Γ_S^V di $[\boldsymbol{\sigma}]$ ci dice quindi che tale orbita si spezza in sottoinsiemi di cardinalità $|H/\mathrm{Inn}(G)|$. Allora deve valere

$$[K^V_{\boldsymbol{\sigma}} : K^V_{\boldsymbol{\sigma}^H}] = (\Gamma^V_{\boldsymbol{\sigma}^H} : \Gamma^V_{\boldsymbol{\sigma}}) = |H/\mathrm{Inn}(G)|.$$

Allora $\mathrm{Gal}(N^H/K^V_{\boldsymbol{\sigma}^H}) \cong H$. □

Teorema 2.41. *Siano G, H, $\mathbf{C}$ e V come nel teorema 2.39, e supponiamo che V possieda un'orbita di lunghezza dispari. Supponiamo inoltre che $\mathbf{C}$ sia V-rigido e che per ogni $\alpha \in H$ esista un $\delta \in \Gamma_{\mathbb{Q}}$ tale per cui $\mathbf{C}^{\alpha V} = \mathbf{C}^{c(\delta)V}$. Allora esiste un'estensione di Galois $N^H/\mathbb{Q}_{\mathbf{C}}^{HV}(\tilde{t})$ tale per cui $N^H/\mathbb{Q}_{\mathbf{C}}^{V}$ è regolare e*

$$\mathrm{Gal}(N^H/\mathbb{Q}_{\mathbf{C}}^{HV}(\tilde{t})) \cong A, \quad \mathrm{Gal}(N^H/\mathbb{Q}_{\mathbf{C}}^{V}(\tilde{t})) \cong \mathrm{Inn}(G).$$

Se $\mathbf{C}$ è HV-simmetrico allora vale inoltre $\mathbb{Q}_{\mathbf{C}}^{HV} = \mathbb{Q}$.

Dimostrazione. Dato che $\mathbf{C}$ è V-rigido e $\mathbf{C}^{HV} \subset \mathbf{C}^{\Gamma V}$ abbiamo che $\Sigma(\mathbf{C}^{\Gamma V})/\mathrm{Inn}(G)$ contiene una sola Γ_S^V-orbita. Allora $\boldsymbol{\sigma}^H \subset [\boldsymbol{\sigma}]^{\Gamma_S^V}$. Si può allora applicare la proposizione 2.40 e ottenere che il campo $K_{\mathbf{C}}^{HV}$ è il campo cercato. Applicando a questo punto il teorema 2.39 e la proposizione 2.35, insieme all'ipotesi di disparità di un'orbita di V, otteniamo che $K_{\boldsymbol{\sigma}^H}^V$ è razionale e soddisfa la formula. □

Teorema 2.42. *Siano G, H, $\mathbf{C}$ e V come nel teorema 2.39, e supponiamo che V possieda un'orbita di lunghezza dispari. Supponiamo che $\Sigma(\mathbf{C}^V)/\mathrm{Inn}(G)$ contenga una A_S^V-orbita rigida su cui agisce H. Esiste allora un'estensione regolare $N^H/\mathbb{Q}_{\mathbf{C}}^{V}(\tilde{z})$ tale che*

$$\mathrm{Gal}(N^H/\mathbb{Q}_{\mathbf{C}}^{V}(\tilde{z})) \cong A, \quad \mathrm{Gal}(N^H/\mathbb{Q}_{\mathbf{C}}^{V}(\tilde{t})) \cong \mathrm{Inn}(G).$$

Se $\mathbf{C}$ è V-simmetrico allora vale inoltre $\mathbb{Q}_{\mathbf{C}}^{V} = \mathbb{Q}$.

Dimostrazione. Sia $[\boldsymbol{\sigma}]^{A_S^V}$ la A_S^V-orbita rigida. Per ipotesi $\sigma^H \subset [\boldsymbol{\sigma}]^{A_S^V}$, mentre per rigidità $[\boldsymbol{\sigma}]^{A_S^V} = [\boldsymbol{\sigma}]^{\Gamma_S^V}$. Possiamo allora applicare la proposizione 2.40 per trovare un'estensione N^H con $\mathrm{Gal}(N^H/K_{\boldsymbol{\sigma}^H}^V) \cong H$ con N^H regolare su $K_{\boldsymbol{\sigma}}^V$. Dall'inclusione fra le orbite sopra scritta otteniamo

$$[K_{\boldsymbol{\sigma}}^V : K_{\boldsymbol{\sigma}^H}^V] = (\Gamma_{\boldsymbol{\sigma}^H}^V : \Gamma_{\boldsymbol{\sigma}}^V) = (A_{\boldsymbol{\sigma}^H}^V : A_{\boldsymbol{\sigma}}^V) = [\overline{\mathbb{Q}}(t)K_{\boldsymbol{\sigma}}^V : \overline{\mathbb{Q}}(t)K_{\boldsymbol{\sigma}^H}^V]$$

quindi $K_{\boldsymbol{\sigma}}^V$ è regolare su $K_{\boldsymbol{\sigma}^H}^V$. D'altra parte per rigidità ricaviamo dal teorema 2.30 che $K_{\boldsymbol{\sigma}}^V$ è regolare su $\mathbb{Q}_{\mathbf{C}}^V$, quindi lo è anche $K_{\boldsymbol{\sigma}^H}^V$. L'ipotesi di disparità dice a questo punto che $K_{\boldsymbol{\sigma}}^V$ è razionale, quindi per Lüroth anche $K_{\boldsymbol{\sigma}^H}^V$. □

Capitolo 3

Composizioni

Tramite i criteri di rigidità esposti è possibile costruire G-realizzazioni per svariati gruppi; vedremo ora, calandoci nel contesto più generale del problema di *immersione*, come sia possibile trovare realizzazioni mettendo insieme quelle già ottenute.

3.1 Problemi di immersione

Definizione 3.1. Un *problema di immersione* è un'estensione di Galois finita L/K e un omomorfismo surgettivo $\phi : H \to \mathrm{Gal}(L/K)$; una *soluzione* del problema di immersione è un'estensione M/K contenente L con un isomorfismo $\psi : H \to \mathrm{Gal}(M/K)$ tale che $\phi = \mathrm{res}^M_L \circ \psi$.

Risolvere un problema di immersione è ovviamente più complesso che risolvere il generico problema inverso, poiché quest'ultimo si riconduce al primo quando l'estensione data è banale. D'altra parte è estremamente semplice mostrare casi in cui il problema di immersione non ha soluzione. Presentiamo brevemente un esempio classico di problema non risolvibile.

Proposizione 3.2. *Supponiamo che esista $d \in K \setminus K^2$ (quindi $\mathrm{char}(K) \neq 2$). Il problema di immersione dato dall'unica mappa surgettiva $\phi : Z_4 \to \mathrm{Gal}(K(\sqrt{d})/K)$ è risolubile se e soltanto se d è somma di due quadrati in K.*

Dimostrazione. Sia L/K una soluzione. Vale $L = K(\sqrt{d}, \sqrt{c})$ con $c = a + b\sqrt{d}$ per opportuni $a, b \in K$; in particolare possiamo scrivere $L = K(\sqrt{a + b\sqrt{d}})$. Possiamo rapidamente calcolare il polinomio minimo di $\sqrt{c}$ su K:

$$p(x) := x^4 - 2ax^2 + (a^2 - db^2) = (x^2 - (a + b\sqrt{d}))(x^2 - (a - b\sqrt{d})).$$

Innanzitutto l'estensione risultante è di Galois se e soltanto se $y_1 := \sqrt{a + b\sqrt{d}}$ e $y_2 := \sqrt{a - b\sqrt{d}}$ generano la stessa estensione di $K(\sqrt{d})$; tale condizione è soddisfatta se e soltanto se il prodotto $y_1^2 y_2^2$ è un quadrato in $K(\sqrt{d})$:

$$y_1 = e + f y_2 \leftrightarrow y_1^2 = a^2 + b^2 y_2^2 + 2aby_2 \leftrightarrow$$
$$a = 0, b \neq 0 \quad y_1^2 = b^2 y_2^2 \leftrightarrow a = 0, b \neq 0 y_1^2 y_2^2 = (by_2^2)^2.$$

Deve quindi essere $s := y_1^2 y_2^2 = (a^2 - db^2)$ quadrato in $K(\sqrt{d})$.

Sia ora σ un automorfismo. Se $\sigma(y_1) = \pm y_1$ ha ordine al più 2; pertanto studiamo il caso $\sigma(y_1) = y_2$, dove abbiamo $\sigma(y_2) = \pm y_1$. Tale automorfismo ha ordine 4 se e soltanto se $\sigma(y_2) = -y_1$, e dall'equazione

$$\sigma(\sqrt{s}) = \sigma(y_1 y_2) = \pm y_1 y_2 = \pm\sqrt{s}$$

ricaviamo quindi che ha ordine 4 se e soltanto se la sua azione su $\sqrt{s}$ non è banale. Quindi se ha ordine 4 troviamo che s non è un quadrato in K.

Se invece il gruppo non è ciclico, ovvero se $\sigma(y_2) = y_1$, $\sqrt{s}$ è fissato da σ; ma anche l'automorfismo $y_1 \mapsto -y_1$ fissa $\sqrt{s}$ e pure $y_1 \mapsto -y_2$ che è composizione dei precedenti. Questo implica che $\sqrt{s} \in K$, quindi s quadrato in K. In sintesi $\mathrm{Gal}(L/K)$ è ciclico se e soltanto se s è un quadrato di $K(\sqrt{d})$ ma non in K. Scrivendo esplicitamente la relazione:

$$a^2 - db^2 = (e + f\sqrt{d})^2 = e^2 + df^2 + 2ef\sqrt{d}$$

otteniamo che $a^2 - db^2 = e^2$ oppure $a^2 - db^2 = df^2$. Per concludere notiamo quindi che se $\mathrm{Gal}(L/K)$ è ciclico

$$d = \left(\frac{a}{f}\right)^2 + \left(\frac{b}{f}\right)^2.$$

Viceversa se d è una somma di quadrati si può scrivere nella forma qui sopra, quindi $\sqrt{a + b\sqrt{d}}$ ci fornisce l'estensione ciclica richiesta. □

Quindi su $\mathbb{Q}$ è sufficiente, per esempio, prendere $d < 0$ per avere infiniti esempi di problemi di immersione non risolvibili.

Definizione 3.3. Si dice *kernel* di un problema di immersione il kernel del relativo omomorfismo ϕ.

Definizione 3.4. Un problema di immersione si dice *spezzato* se il gruppo H che si mappa su $\mathrm{Gal}(L/K)$ si spezza nel prodotto semidiretto del kernel e di $\mathrm{Gal}(L/K)$.

Definizione 3.5. Un problema di immersione si dice *abeliano* se il suo kernel è abeliano.

Osservazione 3.6. Se $\phi : H \to \mathrm{Gal}(L/K)$ è un problema di immersione con kernel U, e U_0 è un sottogruppo normale di H contenuto in U, allora è risolvibile se e soltanto se sono risolvibili i problemi $\phi_0 : H/U_0 \to \mathrm{Gal}(L/K)$ e, fissata una soluzione di quest'ultimo problema $\psi_0 : H/U_0 \to \mathrm{Gal}(M_0/K)$, $\psi_0 \circ \pi : H \to \mathrm{Gal}(M_0/K)$.

Quest'ultima osservazione ci permette di ridurre i problemi di immersione ai casi in cui il kernel non abbia sottogruppi che siano normali in tutto H, ovvero ai casi in cui il kernel sia un sottogruppo normale minimale.

Lemma 3.7. *Se U è un sottogruppo normale minimale di un gruppo finito H allora è isomorfo al prodotto diretto S^m di $m \geq 1$ copie di un gruppo semplice S.*

Dimostrazione. Sia U minimale. Esso conterrà un sottogruppo minimale normale U_0 in U; se $U_0 = U$ allora U è semplice e abbiamo ottenuto la tesi con $S = U$ e $m = 1$. Se invece $U_0 \neq U$ allora i coniugati U_0^h al variare di $h \in U$ sono sottogruppi normali minimali di U; per minimalità, l'intersezione di una coppia distinta di due di essi è banale, quindi commutano fra di loro. Il gruppo generato da tutti gli U_0^h è necessariamente U, altrimenti sarebbe un sottogruppo normale di H più piccolo; esiste quindi un omomorfismo dal prodotto diretto degli U_0^h distinti surgettivo su U.

Dato che abbiamo supposto $U_0 \neq U$ possiamo assumere per ipotesi induttiva che sia $U_0 \cong S^l$ con S semplice e $l \geq 1$. Il prodotto diretto degli U_0^h sarà allora isomorfo ad un prodotto diretto S^n; un suo quoziente sarà allora isomorfo a U tramite la mappa costruita in precedenza. Se S è abeliano è della forma Z_p, quindi U è un gruppo abeliano con elementi di ordine p e pertanto è della forma Z_p^m per il teorema di struttura dei gruppi abeliani. Per il caso non abeliano possiamo invece fare un ragionamento più forte: dimostreremo che ogni sottogruppo normale $N \lhd S^n$ è il prodotto diretto di alcune componenti S, quindi anche che il quoziente S^n/N è sempre della forma S^m. Procediamo per induzione su n.

Il passo $n = 1$ è evidente, se N è sottogruppo normale di S o è S o è banale. Nel caso generale sia π_i la proiezione sulla componente i-esima; se $\pi_i(N)$ è il gruppo banale allora N è un sottogruppo di S^{n-1}, scartando la componente i, e possiamo applicare l'ipotesi induttiva. Altrimenti $\pi_i(N)$ possiede un elemento non banale, quindi N contiene un elemento $(a_1, \dots, a_i, \dots, a_n)$ con $a_i \neq e$. Se $g \in S$ è un elemento qualsiasi per il quale $ga_ig^{-1} \neq a_i$, che esiste sicuramente in quanto altrimenti a_i sarebbe nel centro di S che per ipotesi di semplicità è banale, allora coniugando per $(e, \dots, g, \dots, e)$ otteniamo un vettore $(a_1, \dots, ga_ig^{-1}, \dots, a_n) \in N$. In particolare allora moltiplicando un vettore per l'inverso dell'altro otteniamo $(e, \dots, b, \dots, e) \in N$ con $b \neq e$. Questo implica che N interseca la componente i-esima in un sottogruppo normale non banale, quindi in tutto S. □

3.2 Prodotti a ghirlanda

Definizione 3.8. Sia Γ un gruppo che agisce sull'insieme $\{1, \dots, m\}$ e G_1 un gruppo. Il *prodotto a ghirlanda* di G_1 e Γ, indicato con $G_1 \wr_m \Gamma$ è il prodotto semidiretto $G_1^m \rtimes \Gamma$, con G_1^m prodotto diretto di m copie di G_1, e l'azione di Γ determinata da $(g_1, \dots, g_m)^\gamma = (g_{\gamma^{-1}(1)}, \dots, g_{\gamma^{-1}(m)})$.

Stabiliamo la convenzione d'ora in poi per cui G_1 è visto come sottogruppo di $G_1 \wr_m \Gamma$ identificandolo con la prima componente di G_1^m. Con questa convenzione l'elemento $\gamma g \gamma^{-1}$ è $(e, \dots, e, g, e, \dots, e)$, con g nella posizione $\gamma(1)$.

Lemma 3.9. *Sia H il prodotto a ghirlanda di G_1 e Γ, con Γ che agisce transitivamente su $\{1, \dots, m\}$. Sia Γ_1 lo stabilizzatore di 1 in Γ. Allora per qualunque gruppo H' con sottogruppi G_1' e Γ' tali per cui vi siano due omomorfismi $\phi : G_1 \to G_1'$ e $\psi : \Gamma \to \Gamma'$ con le seguenti proprietà:*

(1) G_1' commuta con $\psi(\gamma) G_1' \psi(\gamma^{-1})$ per ogni $\gamma \in \Gamma \setminus \Gamma_1$;

(2) $\psi(\gamma)$ *commuta con* G_1' *per ogni* $\gamma \in \Gamma_1$*;*

gli omomorfismi si estendono in modo unico ad un omomorfismo $\varphi : H \to H'$*.*

Dimostrazione. Siano $\gamma_i \in \Gamma$ elementi tali per cui $\gamma_i(1) = i$. Allora ogni elemento può essere scritto in modo unico come

$$(g_1, \dots, g_m) \cdot \gamma = \gamma_1 g_1 \gamma_1^{-1} \cdots \gamma_m g_m \gamma_m^{-1} \cdot \gamma$$

con $g_1, \dots, g_m \in G_1$ e $\gamma \in \Gamma$. Con questa scrittura è possibile definire la funzione $\varphi : H \to H'$

$$\varphi((g_1, \dots, g_m) \cdot \gamma) := \psi(\gamma_1)\phi(g_1)\psi(\gamma_1^{-1}) \cdots \psi(\gamma_m)\phi(g_m)\psi(\gamma_m^{-1}) \cdot \psi(\gamma).$$

Per verificare che sia un omomorfismo scriviamo esplicitamente un prodotto:

$$\begin{aligned} hh' &= (\gamma_1 g_1 \gamma_1^{-1} \cdots \gamma_m g_m \gamma_m^{-1} \cdot \gamma) \cdot (\gamma_1' g_1' \gamma_1'^{-1} \cdots \gamma_m' g_m' \gamma_m'^{-1} \cdot \gamma') \\ &= (\gamma_1 g_1 \gamma_1^{-1} \cdot \gamma\gamma_{i_1} g_{i_1}' \gamma_{i_1}^{-1}\gamma^{-1}) \cdots (\gamma_m g_m \gamma_m^{-1} \cdot \gamma\gamma_{i_m} g_{i_m}' \gamma_{i_m}^{-1}\gamma^{-1}) \cdot (\gamma\gamma') \end{aligned}$$

dove i_j è l'indice tale per cui $\gamma\gamma_{i_j}(1) = j$. In particolare abbiamo che $\gamma\gamma_{i_j} \in \gamma_j\Gamma_1$. Dato che però Γ_1 commuta con G_1 per costruzione, otteniamo la scrittura:

$$hh' = \gamma_1(g_1 g_{i_1}')\gamma_1^{-1} \cdots \gamma_m(g_m g_{i_m}')\gamma_m^{-1} \cdot \gamma\gamma'.$$

Per ipotesi anche $\psi(\Gamma_1)$ commuta con $\phi(G_1)$, mentre i vari $\psi(\gamma_i)\phi(G_1)\psi(\gamma_i^{-1})$ commutano fra di loro quando i γ_i non sono nella stessa classe modulo Γ_1, quindi gli stessi riordinamenti fatti sopra si possono ripetere dopo l'applicazione di φ. In questo modo otteniamo che φ è un omomorfismo. □

Corollario 3.10. *Se* G *è un gruppo abeliano e* Γ *un gruppo finito di cui si considera l'azione regolare su* $\{1, \dots, |\Gamma|\}$*, allora ogni prodotto semidiretto* $H = G \rtimes \Gamma$ *è isomorfo ad un quoziente di* $G \wr_{|\Gamma|} \Gamma$*.*

Dimostrazione. Basta notare che esistono due mappe naturali (surgettive) $\phi : G \to \Gamma$ e $\psi : \Gamma \to \Gamma$, con la proprietà che $\psi(\gamma)\phi(G)\psi(\gamma^{-1}) = \phi(G)^{\psi(\gamma)} = \phi(G)$; per abelianità allora è rispettata la condizione (1). Inoltre lo stabilizzatore di 1 è il gruppo banale, poiché la rappresentazione regolare è fedele e transitiva; pertanto è rispettata anche la condizione (2), quindi esiste un omomorfismo surgettivo da $G \wr_{|\Gamma|} \Gamma$ a H. In particolare H è isomorfo al quoziente del prodotto a ghirlanda per il kernel dell'omomorfismo. □

Il prodotto a ghirlanda si presta per la costruzione di occorrenze regolari di gruppi; il principio è quello di aggiungere variabili trascendenti in modo da procurarsi la realizzazione di un prodotto di più copie di un gruppo già realizzato, poi di permutare le nuove variabili fra di loro in modo da ottenere il prodotto cercato. Stabiliamo prima un risultato preliminare che ci sarà indispensabile nella successiva costruzione.

Lemma 3.11. *Sia* l/k *un'estensione finita di Galois e* Γ *un gruppo di automorfismi di* $L = l(x_1, \dots, x_s)$ *con* $x_1, \dots, x_s$ *algebricamente indipendenti su* l*. Supponiamo che*

l sia invariante in L per l'azione di Γ e che la restrizione di tale azione fornisca un isomorfismo di Γ con $\mathrm{Gal}(l/k)$. Se lo spazio vettoriale generato da $x_1, \dots, x_s$ su l è Γ-invariante, allora il campo fisso di Γ è puramente trascendente su k:

$$L^\Gamma = k(t_1, \dots, t_s)$$

con $t_1, \dots, t_s$ algebricamente indipendenti su k. I $t_1, \dots, t_s$ possono essere scelti in modo da formare una base su l dello spazio generato dagli $x_1, \dots, x_s$ su l.

Dimostrazione. Sia $\Omega := \langle x_1, \dots, x_s \rangle_l$. Lo spazio Ω^Γ è naturalmente uno spazio vettoriale su k; prendiamo allora in esso $t_1, \dots, t_h$ vettori k-linearmente indipendenti. Se tali vettori fossero l-linearmente dipendenti, vi sarebbe una scelta di coefficienti tali che $\sum_i a_i t_i = 0$ con almeno un $a_i = 1$. Calcolandone la traccia i vettori t_i restano fissi per costruzione, pertanto otteniamo una combinazione lineare $\sum_i T_k^l(a_i) t_i = 0$, con almeno un coefficiente uguale a $|\Gamma| \neq 0$. Quindi sono anche l-linearmente indipendenti.

Fissiamo ora un generatore α di l/k. Prediamo un qualsiasi $u \in \Omega$ e scriviamo

$$u_i := \sum_{\gamma \in \Gamma} \gamma(\alpha)^{i-1} \gamma(u)$$

con $n = |\Gamma|$. La matrice $(\gamma(\alpha)^{i-1})$ è una matrice di Vandermonde calcolata sui coniugati di α che sono tutti distinti, quindi in particolare è invertibile. Da questo ricaviamo che i vettori $\gamma(u)$ sono combinazioni a coefficienti in l dei vettori u_i; ma tali u_i sono fissati dall'azione di Γ per costruzione, quindi giacciono in Ω^Γ. In particolare allora u è combinazione l-lineare di vettori di Ω^Γ.

Per arbitrarietà di u deduciamo quindi che una base come k-spazio vettoriale di Ω^Γ genera su l tutto Ω ed è di vettori l-linearmente indipendenti, quindi è anche una l-base di Ω. Fissiamo quindi l'automorfismo l-lineare ϕ per il quale $\phi(x_i) = t_i$.

Esiste allora un unico modo di estendere ϕ ad un automorfismo di campo di L; in particolare otteniamo $L = l(t_1, \dots, t_s)$ con $t_1, \dots, t_s$ algebricamente indipendenti su l (se lo fossero lo sarebbero anche gli $x_1, \dots, x_s$). Il campo L^Γ contiene certamente $k(t_1, \dots, t_s)$, mentre $[L : k(t_1, \dots, t_s)] = [l(t_1, \dots, t_s) : k(t_1, \dots, t_s)] = [l : k] = |\Gamma| = [L : L^\Gamma]$. Quindi $L^\Gamma = k(t_1, \dots, t_s)$. □

Proposizione 3.12. *Sia l/k un'estensione normale finita, Γ il suo gruppo di Galois e Γ_1 un suo sottogruppo con campo fisso l_1. Sia $m := [\Gamma : \Gamma_1]$ e sia data una rappresentazione di permutazione transitiva di Γ su $\{1, \dots, m\}$ in modo che Γ_1 sia lo stabilizzatore di 1. Sia poi G_1 un gruppo finito che occorre regolarmente su l_1, sia H il prodotto a ghirlanda $G_1 \wr_m \Gamma$ e $\pi : H \to \Gamma$ la proiezione canonica.*

Esiste allora un vettore $\mathbf{t} := t_1, \dots, t_M$ di elementi algebricamente indipendenti su l, un'estensione $L/l(\mathbf{t})$ regolare su l e di Galois su $k(\mathbf{t})$ e un isomorfismo $\phi : H \to \mathrm{Gal}(L/k(\mathbf{t}))$ per il quale $\mathrm{res}_l^L \circ \phi = \pi$.

Inoltre, se in H esiste un sottogruppo normale N tale per cui $G_1^m \cdot N = H$, allora H/N occorre regolarmente su k.

Dimostrazione. Supponiamo che $K_1/l_1(\mathbf{x}_1)$ sia una realizzazione regolare di G_1, con $\mathbf{x}_1$ vettore di elementi algebricamente indipendenti su l_1, quindi anche su

l. Sia $\mathbf{x} = (x_1, \dots, x_M)$ un vettore di elementi algebricamente indipendenti su l che estenda $\mathbf{x}_1$, partizionato in vettori $\mathbf{x}_1, \dots, \mathbf{x}_m$ ognuno della stessa lunghezza. Poniamo che l'azione di Γ sugli elementi di $\mathbf{x}$ permuti le partizioni $\mathbf{x}_1, \dots, \mathbf{x}_m$ come $\gamma(\mathbf{x}_i) = \mathbf{x}_{\gamma(i)}$. Imponiamo inoltre che Γ_1 lasci puntualmente fisso il vettore $\mathbf{x}_1$.

Estendiamo nuovamente $\mathbf{x}$ con gli elementi $y_1, \dots, y_m$ in modo che siano ancora tutti algebricamente indipendenti su l. Poniamo che Γ agisca sugli y_i come $\gamma(y_i) = y_{\gamma(i)}$.

Ora estendiamo l'azione di Γ su tutto l'anello $l(\mathbf{x})[y_1, \dots, y_m]$. Sia $f_1(\mathbf{x}_1, y_1) \in l_1(\mathbf{x}_1)[y_1]$ che generi l'estensione $K_1/l(\mathbf{x}_1)$, ossia per il quale si abbia $K_1 \cong l_1(\mathbf{x}_1)[y_1]/(f_1)$. Definiamo poi $f_i(\mathbf{x}_i, y_i) := \gamma(f_1)$ per $\gamma(1) = i$ (tale definizione è buona poiché se due γ coincidono su 1, differiscono per un elemento di Γ_1 che per costruzione agisce banalmente su $l_1(\mathbf{x}_1)[y_1]$). Tali polinomi restano tutti irriducibili su $l(\mathbf{x})$ per il lemma 1.11. Poniamo

$$L := l(\mathbf{x})[y_1, \dots, y_m]/(f_1, \dots, f_m).$$

L'azione di Γ si trasferisce in modo naturale su L. Notiamo che L è un'estensione regolare, poiché è di fatto il composto in una chiusura algebrica di $l(\mathbf{x})$ di estensioni K_i regolari su l. Essendo inoltre tutte estensioni normali essa è un'estensione normale di $l(\mathbf{x})$. Notiamo che il suo gruppo di Galois $G := \mathrm{Gal}(L/l(\mathbf{x}))$ contiene m sottogruppi G_i che definiamo come i gruppi di automorfismi che fissato $\overline{y}_j$ per ogni $j \neq i$. Ognuno di questi sottogruppi ha intersezione banale con gli altri, mentre ognuno di essi è isomorfo a G_1 per costruzione; inoltre commutano evidentemente fra di loro. Quindi $\prod_i G_i \subset G$, e dal raffronto dei gradi otteniamo proprio $G = \prod_i G_i \cong G_1^m$.

L'azione di Γ su L è tale che $\gamma(\overline{y}_i) = \overline{y}_{\gamma(i)}$; dato che $\Gamma(l(\mathbf{x})) = l(\mathbf{x})$ possiamo scrivere $\gamma G_i \gamma^{-1} = G_{\gamma(i)}$. In particolare abbiamo che G_1 commuta con $\gamma G_1 \gamma^{-1}$ ogni volta che $\gamma \in \Gamma \setminus \Gamma_1$.

Se $\gamma \in \Gamma_1$ invece esso agisce in modo banale su $l_1(\mathbf{x}_1)(\overline{y}_1)$; in particolare allora γ lascia fisso tutti i coniugati di $\overline{y}_1$, pertanto $\gamma g \gamma^{-1}(\overline{y}_1) = g(\overline{y}_1)$ per ogni $g \in G_1$. Quindi in particolare $\gamma g \gamma^{-1} = g$, ossia Γ_1 commuta con G_1.

Per il lemma 3.9 esiste quindi un unico omomorfismo ϕ dal prodotto $H = G_1 \wr_m \Gamma$ in $\mathrm{Aut}(L)$, dove G_1 e Γ sono mappati identicamente in se stessi. L'immagine H' di questo omomorfismo è generata dall'immagine di G_1^m, che di fatto è $\prod_i G_i = \mathrm{Gal}(L/l(\mathbf{x}))$, e da Γ, quindi il suo campo fisso $L^{H'}$ è l'intersezione di $l(\mathbf{x})$ e del campo fisso di Γ, cioè $l(\mathbf{x})^\Gamma$. Per calcolare quest'ultimo campo possiamo applicare il lemma 3.11 e ottenere che è della forma $k(\mathbf{t})$ con $\mathbf{t}$ vettore di M elementi algebricamente indipendenti su l. In sintesi $H' = \mathrm{Gal}(L/k(\mathbf{t}))$. Notiamo infine che per confronto di ordini H' è di fatto isomorfo ad H, mentre $\phi(G_1^m) = \mathrm{Gal}(L/l(\mathbf{x}))$ implica che $\mathrm{res}_l^L \circ \phi$ è banale su $\phi(G_1^m)$, quindi che in effetti $\mathrm{res}_l^L \circ \phi = \phi$.

Se N è un sottogruppo normale di H tale che $G_1^m \cdot N = H$, allora $L^N \cap l(\mathbf{x}) = k(\mathbf{t})$. In particolare allora L^N è regolare su k e fornisce un'occorrenza di H/N in quanto $H/N \cong \mathrm{Gal}(L^N/k(\mathbf{t}))$. □

Corollario 3.13. *Sia H il prodotto a ghirlanda di G_1 e Γ, con Γ che agisce transitivamente su $\{1, \dots, m\}$.*

(a) *Se G_1 e Γ occorrono regolarmente su un campo k, allora occorre regolarmente anche H.*

(b) *Sia $\pi : H \to \Gamma$ la proiezione naturale. Se k è hilbertiano, l/k è un'estensione con gruppo di Galois Γ e G_1 occorre regolarmente su k allora il problema di immersione dato da π su k ha soluzione.*

Dimostrazione. (a) Sia $\mathbf{y}$ un vettore di elementi algebricamente indipendenti su k tale per cui si abbia un'estensione L/K, con $K = k(\mathbf{y})$, regolare su k e con gruppo di Galois Γ. Sia Γ_1 lo stabilizzatore di 1 in Γ; sul campo fisso $l_1 := L^{\Gamma_1}$ occorre regolarmente G_1 per il lemma 1.11. Possiamo quindi applicare la proposizione 3.12 per ottenere un vettore di elementi algebricamente indipendenti su K tale per cui $H \cong \mathrm{Gal}(L'/K(\mathbf{t}))$ per un opportuno L' regolare su L. In particolare $L' \cap \overline{k} = L' \cap \overline{L} \cap \overline{k} = L \cap \overline{k} = k$, e unito al fatto che L' è un'estensione di $k(\mathbf{y}, \mathbf{t})$ che è puramente trascendente su k otteniamo che H occorre regolarmente su k.

(b) La proposizione 3.12 ci fornisce un isomorfismo $\phi : H \to \mathrm{Gal}(L/k(\mathbf{t}))$. Se k è hilbertiano esiste una specializzazione delle variabili trascendenti tale per cui un polinomio che generi l'estensione resti irriducibile; in particolare $H \cong \mathrm{Gal}(L'/k)$. Basta osservare che $L \cap \overline{k} = l$ per dedurre che la specializzazione è un isomorfismo quando ristretta a l, e in particolare che anche il suo gruppo di Galois viene mappato isomorficamente in $\mathrm{Gal}(L'/k)$. Di conseguenza l'isomorfismo $\tilde{\phi}$ indotto dalla specializzazione ha la proprietà che $\mathrm{res}^{L'}_{l} \circ \tilde{\phi} = \pi$. □

Corollario 3.14. *(a) Ogni gruppo abeliano finito occorre regolarmente su k.*

(b) *Sia $H = G_1 \rtimes \Gamma$, con G_1 abeliano. Se Γ occorre regolarmente su k anche H occorre regolarmente su k.*

(c) *Se k è hilbertiano ogni problema di immersione abeliano spezzato su k ha soluzione.*

Dimostrazione. (a) Innanzitutto procuriamoci una realizzazione per tutti i gruppi ciclici. Sia allora $n \geq 2$ un intero fissato. Sia l/k l'estensione di k costruita aggiungendo la radice n-esima dell'unità (eventualmente già in k); il gruppo Z_n occorre regolarmente su l in quanto gruppo di Galois di $l(x)/l(x^n)$.

Poniamo ora $\Gamma = \mathrm{Gal}(l/k)$ e consideriamo la rappresentazione regolare di permutazione di Γ su $\{1, \ldots, |\Gamma|\}$ e poniamo $H := Z_n \wr_{|\Gamma|} \Gamma$. Esiste allora per il lemma 3.9 un omomorfismo da H in Z_n che sia l'identità su Z_n e banale su Γ. Il suo kernel N ci fornisce un sottogruppo normale di H tale per cui $Z_n^{|\Gamma|} \cdot N = H$; unendo questo al fatto che lo stabilizzatore di 1 in Γ è banale possiamo applicare la proposizione 3.12 e ottenere che Z_n occorre regolarmente su k.

Ricordiamo ora che per il corollario 3.10 ogni prodotto semidiretto con fattore normale abeliano, in particolare anche diretto, è isomorfo ad un quoziente di un prodotto a ghirlanda; per il corollario 3.13 se G_1 e G_2 sono due gruppi abeliani che occorrono regolarmente su k anche il loro prodotto a ghirlanda occorre regolarmente su k come pure tutti i suoi quozienti; in particolare anche il prodotto diretto. Per concludere basta usare il teorema di struttura dei

gruppi abeliani finiti e spezzare ogni gruppo abeliano in prodotto diretto di gruppi ciclici.

(b) Di nuovo per il corollario 3.10 il prodotto semidiretto si può scrivere come quoziente di un prodotto a ghirlanda dei due fattori; dato che entrambi occorrono regolarmente su k, anche il prodotto richiesto occorre regolarmente su k.

(c) Sia $\phi : H \to \Gamma = \mathrm{Gal}(l/k)$ con kernel abeliano G_1. Per ipotesi G_1 ha un complementare in H isomorfo a Γ tramite ϕ; esiste allora un omomorfismo π, per il corollario 3.10, da $H' := G_1 \wr_{|\Gamma|} \Gamma$ su H che sia surgettivo. Per il corollario 3.13 esiste un'estensione L'/k che risolve il problema di immersione $\phi' := \phi \circ \pi$. Restringendosi ora al campo fisso del kernel di π otteniamo evidentemente una soluzione del problema di immersione originale. □

3.3 Realizzazioni GAR e GAL

Abbiamo appena visto un criterio generale per la soluzione di problemi di immersione abeliani, cioè che sono risolubili ogni qualvolta sono problemi di tipo spezzato. Vediamo ora invece come si possano formulare dei criteri, uno dei quali sarà di rigidità, con cui assicurare l'esistenza di soluzioni a problemi di immersione con kernel non abeliani.

Nostro scopo sarà risolvere problemi minimali, pertanto con kernel della forma S^m con S semplice non abeliano; ci restringeremo quindi a parlare di gruppi con centro banale.

Definizione 3.15. Sia G un gruppo finito con centro banale. Una G-realizzazione di G della forma $K/k(\mathbf{x})$ è detta *GA-realizzazione* se esiste un sottocampo $k \subset F \subset k(\mathbf{x})$ tale per cui $\mathrm{Gal}(K/F) \cong \mathrm{Aut}(G)$ e il sottogruppo $\mathrm{Inn}(G)$ è identificato, nell'isomorfismo, con $\mathrm{Gal}(K/k(\mathbf{x}))$.

Tale realizzazione è detta GAR-realizzazione se soddisfa anche la condizione per cui ogni sottocampo $F \subset R \subset \bar{k}(\mathbf{x})$ con $\bar{k}R = \bar{k}(\mathbf{x})$ è puramente trascendente su $\tilde{k} = k \cap R$.

Una GA-realizzazione è invece detta GAL-realizzazione se il k-spazio vettoriale generato da $\mathbf{x}$ è invariante per l'azione di $\mathrm{Gal}(k(\mathbf{x})/F)$.

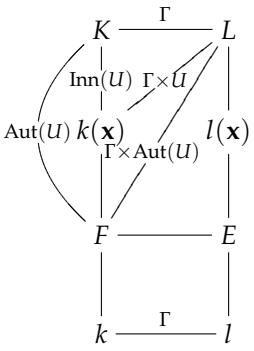
Possiamo enunciare per gruppi con GAR-realizzazioni un risultato analogo alla proposizione 3.12.

Proposizione 3.16. *Sia l/k un'estensione finita, Γ il suo gruppo di Galois, $\varphi : H \to \Gamma$ un omomorfismo surgettivo fra gruppi finiti con kernel U. Supponiamo che U abbia una GAR-realizzazione su k. Allora esiste un vettore di elementi algebricamente indipendenti $\mathbf{t} = (t_1, \ldots, t_s)$ su l, un'estensione $L/l(\mathbf{t})$ regolare su $\mathbf{t}$ e di Galois su $k(\mathbf{t})$ ed un isomorfismo $\phi : H \to \mathrm{Gal}(L/k(\mathbf{t}))$ con $\mathrm{res}^L_l \circ \phi = \varphi$.*

Dimostrazione. Siano K, $k(\mathbf{x})$ ed F campi che forniscano una GAR-realizzazione di U. Siano $L := Kl$ e $F' := Fl$. Dato che K è regolare su k, vale $K \cap l(\mathbf{x})$, quindi $\mathrm{Gal}(L/k(\mathbf{x})) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/l(\mathbf{x})) \cong \Gamma \times U$. In particolare $\mathrm{Gal}(L/K)$ è isomorfo a $\mathrm{Gal}(l/k) = \Gamma$ attraverso la restrizione su l. Otteniamo da questo che F' è invariante per l'azione di $\mathrm{Gal}(L/K)$, quindi quest'ultimo gruppo si mappa

in $\mathrm{Aut}(F'/F)$; in particolare, la mappa è iniettiva, quindi $\mathrm{Aut}(F'/F)$ contiene almeno $|\Gamma| = [l : k]$ elementi. Dato però che $[F' : F] \leq [l : k]$ otteniamo che F' è di Galois su F con gruppo di automorfismi isomorfo a Γ. Otteniamo quindi un isomorfismo

$$\phi_1 : \mathrm{Gal}(L/F) = \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/F') \to \Gamma \times \mathrm{Aut}(U).$$



Costruiamo inoltre l'omomorfismo $\phi_0 : H\Gamma \times \mathrm{Aut}(U)$ che mappa $h \mapsto (\phi(h), \iota_h)$, dove con ι_h intendiamo l'automorfismo $i_h(u) = huh^{-1}$. Quest'omomorfismo è iniettivo: $\ker(\phi_0) = \ker(\phi) \cap \mathcal{C}_H(U) = U \cap \mathcal{C}_H(U) = Z(U) = \{e\}$. Definiamo quindi $\phi := \phi_1^{-1} \circ \phi_0$, che sarà un omomorfismo iniettivo da H in $\mathrm{Gal}(L/F)$, $H' := \phi(H)$ e $R := L^{H'}$. Vale ovviamente $F \subset R$.

Osserviamo ora che $\Gamma \times \mathrm{Aut}(U) = \phi_0(H) \cdot (\{e\} \times \mathrm{Aut}(U))$, mentre $\{e\} \times \mathrm{Inn}(U) = \phi_0(H) \cap (\{1\} \times \mathrm{Aut}(U))$ poiché per definizione $U = \ker(\varphi)$. Applicando ϕ_1^{-1} otteniamo

$$\mathrm{Gal}(L/F) = H' \cdot \mathrm{Gal}(L/F'), \qquad \mathrm{Gal}(L/l(\mathbf{x})) = H' \cap \mathrm{Gal}(L/F')$$

dalle quali ricaviamo

$$F = R \cap F', \qquad l(\mathbf{x}) = RF' = RFl = Rl.$$

Otteniamo quindi $R \cap l = R \cap F' \cap l = F \cap l = k$, mentre $R \cap \bar{l} = R \cap L\bar{l} = R \cap l = k$; quindi R è regolare su k. D'altra parte $\bar{k}R = \bar{k}Rl = \bar{k}l(\mathbf{x}) = \bar{k}(\mathbf{x})$. Dalla definizione di GAR-realizzazione otteniamo quindi che R è della forma $k(\mathbf{t})$, con $\mathbf{t}$ collezione di elementi algebricamente indipendenti su k.

Abbiamo quindi costruito un omomorfismo $\phi : H \to \mathrm{Gal}(L/k(\mathbf{t}))$. Calcoliamo ora $\mathrm{res}^L_l \circ \phi$. Per costruzione della mappa ϕ_1, restringersi a l equivale a proiettare sulla prima componente del prodotto diretto, ossia $\mathrm{res}^L_l = \pi_1 \circ \phi_1$. Scrivendo esplicitamente il conto: $res^L_l \circ \phi = \pi_1 \circ \phi_1 \circ \phi = \pi_1 \circ \phi_0 = \varphi$. □

Corollario 3.17. *Si ha che:*

(a) Se k è hilbertiano, ogni problema di immersione il cui kernel ha una GAR-realizzazione ha soluzione.

(b) Sia H un gruppo finito che abbia U come sottogruppo normale. Se H/U occorre regolarmente su k, con $H/U \cong \mathrm{Gal}(K/k(\mathbf{y}))$, e U ha una GAR-realizzazione su $k(\mathbf{y})$, allora H occorre regolarmente su k.

Dimostrazione. (a) La dimostrazione è identica a quella del corollario 3.13; dato un problema $\phi : H \to \mathrm{Gal}(l/k)$, si costruisce tramite la proposizione 3.16 un'estensione $L/k(\mathbf{t})$ con le giuste proprietà sugli isomorfismi, poi si specializza per hilbertianità notando che l viene lasciato intatto dalla specializzazione.

(b) Se U ha una GAR-realizzazione su $k(\mathbf{y})$ allora è possibile, per mezzo della proposizione 3.16, costruire un'estensione $L/k(\mathbf{y}, \mathbf{t})$ con gruppo H regolare su k, con $\mathbf{y}, \mathbf{t}$ di elementi algebricamente indipendenti su k. In particolare quindi H occorre regolarmente su k. □

Le GAR-realizzazioni sono quindi uno strumento piuttosto potente; la proprietà che le definisce è però difficilmente verificabile in modo diretto. Le GAL-realizzazioni sono invece più facilmente verificabili, ed hanno inoltre migliori proprietà di invarianza.

Lemma 3.18. *(a) Se un gruppo U ha una GAL-realizzazione su k, ha una GAL-realizzazione su ogni campo k' contenente k.*

(b) Ogni GAL-realizzazione è anche una GAR-realizzazione.

(c) Se un gruppo U quasi semplice ha una GAL-realizzazione su k, allora anche U^m ha una GAL-realizzazione per ogni $m \geq 1$.

Dimostrazione. (a) Siano K, $k(\mathbf{x})$ e F i campi della GAL-realizzazione di U. Prendendo un polinomio $f(\mathbf{x}, y)$ che generi l'estensione $K/k(\mathbf{x})$, possiamo usarlo per generare un'estensione $K'/k'(\mathbf{x})$ con gruppo di Galois isomorfo (tramite restrizione) grazie al lemma 1.11. L'azione di $Q := \mathrm{Gal}(k(\mathbf{x})/F)$ su $k(\mathbf{x})$ come azione k-lineare si estende in modo unico ad un'azione k'-lineare su $k'(\mathbf{x})$ che sarà quindi anche un automorfismo di campi. Sicuramente abbiamo l'inclusione $F' := Fk' \subset k'(\mathbf{x})^Q$, pertanto $[k'(\mathbf{x}) : F'] \geq |Q| = [k(\mathbf{x}) : F]$, dalla quale ricaviamo, tramite $[K' : k'(\mathbf{x})] = [K : k(\mathbf{x})]$, $[K' : F'] \geq [K : F]$.

Se γ_1 è un generatore di K su F, allora K' è generato su F' da tutti i coniugati di γ_1 su F. In particolare allora K' è di Galois su F', in quanto gli automorfismi che fissano F' fissano anche F e quindi lasciano invariato l'insieme dei coniugati di γ_1; inoltre la restrizione da $\mathrm{Gal}(K'/F')$ a $\mathrm{Gal}(K/F)$ è iniettiva, poiché un automorfismo che lasci fisso K lascia fisso i coniugati di γ_1, quindi anche K'. Unendo questa informazione alla diseguaglianza prima ricavata sui gradi otteniamo che $\mathrm{Gal}(K'/F') \cong \mathrm{Gal}(K/F)$ (tramite restrizione).

In questo modo K', $k'(\mathbf{x})$ e F' sono una GA-realizzazione. Sappiamo però anche che $\mathrm{Gal}(K'/F')$ lascia invariato lo spazio generato da $x_1, \ldots, x_s$ su k, quindi resterà invariato anche generando su k'. Abbiamo ottenuto una GAR-realizzazione su k'.

(b) Siano di nuovo K, $k(\mathbf{x})$ e F i campi della GAL-realizzazione. Sia ora R contenente F e tale che $\overline{k}R = \overline{k}(\mathbf{x})$. In base al ragionamento precedente siamo liberi di estendere k a $\tilde{k} := R \cap \overline{k}$, prendendo $\tilde{F} := \tilde{k}F \subset R$; supponiamo allora per semplicità che sia già $R \cap \overline{k} = k$ senza bisogno di estendere preliminarmente.

Dall'ipotesi $\overline{k}R = \overline{k}(\mathbf{x})$ ricaviamo che ogni x_i è multiplo per un valore di $\overline{k}$ di un elemento di R; in particolare allora possiamo prendere un estensione finita l tale per cui $lR = l(\mathbf{x})$. Assumiamo anche, a meno di prendere la chiusura normale, che l/k sia di Galois. Sappiamo che $l(\mathbf{x})/F$ è di Galois, in quanto composto delle estensioni normali $k(\mathbf{x})/F$ e lF/F; definendo $F' := lF$ troviamo che $F' \cap k(\mathbf{x}) = F$, quindi che $\mathrm{Gal}(l(\mathbf{x})/F) \cong \mathrm{Gal}(l(\mathbf{x})/k(\mathbf{x})) \times \mathrm{Gal}(l(x)/F')$.

Notiamo ora che $\mathrm{Gal}(l(\mathbf{x})/R)$ lascia l invariante, mentre la sua restrizione su l è un isomorfismo con $\mathrm{Gal}(l/k)$, in quanto il suo campo fisso è $R \cap l = k$; inoltre la sua azione ristretta a $k(\mathbf{x})$ lascia invariato lo spazio vettoriale generato dagli $x_1, \ldots, x_s$ su k, quindi, per unicità dell'estensione come azione lineare su l, lascia invariato anche lo spazio generato su l. Possiamo allora applicare il lemma 3.11 e ottenere che R è di fatto puramente trascendente su k, ossia della

forma $R = k(\mathbf{t})$. Quindi la GAL-realizzazione presa in considerazione è una GAR-realizzazione.

(c) Studiamo innanzitutto il gruppo degli automorfismi di U^m. Dato che U è quasi semplice, è un sottogruppo di $\mathrm{Aut}(S)$ contenente $\mathrm{Inn}(S)$, con S gruppo semplice non abeliano; dato che se un elemento $\phi \in \mathrm{Aut}(S)$ commuta con tutto $\mathrm{Inn}(S)$ vale $i_g(\phi(h) = \phi(i_g(h)) = \phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = i_{\phi(g)}(\phi(h))$ per ogni $g, h \in S$, otteniamo $\phi(g) = g$ poiché gli automorfismi interni coincidono, quindi $\phi = \{e\}$. In particolare $Z(U)$ contiene il centralizzatore di $\mathrm{Inn}(S)$, quindi $Z(U) = \{e\}$. Poniamo allora $A = \mathrm{Aut}(U)$ e identifichiamo U con $\mathrm{Inn}(U) < A$.

Consideriamo ora $\tilde{A} = A \wr_m S_m$ il prodotto a ghirlanda con il gruppo simmetrico. Il gruppo U^m si immerge naturalmente in $\tilde{A}$ come sottogruppo normale, mentre il suo centralizzatore è il solo stabilizzatore di 1, pertanto è banale. Possiamo allora immergere $\tilde{A}$ in $\mathrm{Aut}(U^m)$.

Sappiamo inoltre che se prendiamo un sottogruppo N normale in $\mathrm{Aut}(S)$ non banale esso dovrà contenere S; basta infatti calcolare, per un generico $\phi \in N \setminus \{e\}$ e per un $g \in S$ tale che $\phi(g) \neq g$

$$(\iota_g \phi \iota_{g^{-1}} \phi^{-1})(h) = g(\phi(g^{-1}\phi^{-1}(h)g))g^{-1} = (g\phi(g^{-1}))h(g\phi(g^{-1}))^{-1} = \iota_{g\phi(g^{-1})}(h)$$

ovvero $N \ni \iota_g \phi \iota_g^{-1} \phi^{-1} = \iota_{g\phi(g^{-1})} \in S$. Allora $N \cap S$ è un sottogruppo normale non banale di S, quindi S stesso. In questo modo S è l'unico sottogruppo minimale normale di U.

Se ora N è un sottogruppo normale di U^m, abbiamo che se N proiettato su una componente U del prodotto diretto ha immagine non banale contiene il sottogruppo S di tale componente. Se infatti N possiede un qualsiasi elemento $\mathbf{g} = (g_1, \ldots, g_i, \ldots, g_m)$ con $g_i \neq e$, allora ponendo $\mathbf{h} := (e, \ldots, e, h, e, \ldots, e)$ con h nella posizione i otteniamo $\mathbf{hgh}^{-1}\mathbf{g}^{-1} = (e, \ldots, e, hgh^{-1}g^{-1}, e, \ldots, e)$. Basta allora prendere un h che non commuta con g, cosa sicuramente possibile in quanto $Z(S) = \{e\}$. In particolare, allora, i sottogruppi normali minimali sono tutti della forma S, con S sottogruppo minimale di una componente U del prodotto diretto.

Abbiamo allora che S^m, inteso come prodotto dei sottogruppi minimali delle componenti, è invariante per l'azione di $\mathrm{Aut}(U^m)$; inoltre sempre per la considerazione precedente S^m ha m sottogruppi normali massimali, ognuno ottenuto sostituendo una componente del prodotto con il sottogruppo banale, quindi l'azione di $\mathrm{Aut}(U^m)$ può solamente permutare questi sottogruppi. I centralizzatori in $\mathrm{Aut}(U^m)$ di ognuno di tali sottogruppi massimali sono evidentemente le singole componenti U, pertanto $\mathrm{Aut}(U^m)$ permuta i fattori del prodotto diretto; il kernel dell'azione di permutazione è allora A^m. Possiamo allora concludere che $|\mathrm{Aut}(U^m) \leq |A^m| \cdot |S_m| = |\tilde{A}|$, quindi che $\mathrm{Aut}(U^m) = \tilde{A}$.

Prendendo allora una GAL-realizzazione $K/k(\mathbf{x})$ di U costruiamo, con l'identica procedura usata nella proposizione 3.12, un'estensione $\tilde{K}/k(\tilde{\mathbf{x}})$, con $\tilde{\mathbf{x}}$ vettore di m copie $\mathbf{x}_1, \ldots, \mathbf{x}_m$ algebricamente indipendenti di $\mathbf{x}$, che sia il composto di estensioni $K_i/k(\mathbf{x}_i)$ con gruppo di Galois U. Il suo gruppo complessivo sarà U^m.

Sia ora F il sottocampo di $k(\mathbf{x}_1)$ fissato da $\mathrm{Aut}(U)$. Il gruppo $\mathrm{Gal}(K/F)$ si estende ovviamente su $\tilde{K}$, lasciando fisse le varie estensioni K_i per $i \neq 2$.

Facciamo ora agire S_m su $\tilde{K}$ come permutazione dei K_i; allora il lemma 3.9 ci garantisce l'esistenza di un omomorfismo da $\tilde{A}$ in $\mathrm{Aut}(\tilde{K})$. Questo omomorfismo è iniettivo su U^m e S_m; il suo kernel quindi è un sottogruppo normale che interseca U^m nel gruppo banale. Il kernel commuta pertanto con U^m, è contenuto nel gruppo di S_m delle permutazioni banali e quindi è il gruppo banale. Abbiamo quindi che $\mathrm{Aut}(U) \cong \tilde{A}$ si immerge in $\mathrm{Aut}(\tilde{K})$.

L'ultima condizione da verificare è che l'azione di $\tilde{A}$ lasci invariato lo spazio vettoriale generato da $x_1, \dots, x_M$ su k; ma ciò è evidentemente verificato, in quanto A lascia invariato lo spazio generato dagli $x_1, \dots, x_m$ per ipotesi, mentre S_m permuta solamente gli elementi x_i. □

Corollario 3.19. *(a) Sia H un gruppo finito nel quale tutti i fattori di composizione sono non abeliani e hanno una GAL-realizzazione su k. Allora H occorre regolarmente su k.*

(b) Sia U un gruppo quasi semplice con una GAL-realizzazione su k. Allora tutti i problemi di immersione con kernel U^m su $k' \subset k$ hilbertiano hanno soluzione.

Dimostrazione. (a) Se S^m è un sottogruppo minimale di H, S è un fattore di composizione di H, quindi ha una GAL-realizzazione; in particolare allora anche S^m ha una GAL-realizzazione. Supponendo induttivamente che H/S^m occorra regolarmente su k, esiste un'estensione $K/k(\mathbf{x})$ con gruppo H/S^m; allora S^m ha una GAR-realizzazione su $k(\mathbf{x})$ per la proposizione 3.18, quindi in particolare il problema di immersione dato dalla proiezione $H \to H/S^m$ ha soluzione e fornisce una realizzazione regolare di H su $k(\mathbf{x})$. In particolare, H occorre regolarmente su k.

(b) U^m ha in queste ipotesi una GAR-realizzazione su k'; quindi per il corollario 3.17 i problemi di immersione su k' con kernel U^m hanno tutti soluzione. □

È molto semplice verificare l'esistenza di GAL-realizzazioni date delle opportune ipotesi di rigidità.

Proposizione 3.20. *Sia G un gruppo finito con centro banale immerso in $H := \mathrm{Aut}(G)$.*

(a) Se $[H : G] = 2$ e H ha un vettore $\mathbf{C} \in \mathrm{Cl}(H)^3$ rigido razionale, allora G ha una GAL-realizzazione su $\mathbb{Q}$.

(b) Se H/G è ciclico e H ha un vettore $\mathbf{C} \in \mathrm{Cl}(H)^3$ rigido di cui una componente è contenuta in G, allora G ha una GAL-realizzazione su $\mathbb{Q}^{\mathrm{ab}}$.

Dimostrazione. Sia $k = \mathbb{Q}$ nel caso (a) e $k = \mathbb{Q}^{\mathrm{ab}}$ nel caso (b). Sia $S = \{0, 1, \infty\}$ il luogo di ramificazione e K l'estensione di $k(x)$ con gruppo H data dal teorema 2.19. Imponiamo anche che il generatore di un gruppo di inerzia su 1 appartenga alla classe di coniugio contenuta in G, nel caso che sia $k = \mathbb{Q}^{\mathrm{ab}}$.

L'estensione $K^G/k(x)$ è un'estensione ciclica di grado $n := [H : G]$. Nel caso $n = 2$ l'estensione è quadratica, quindi della forma $k(z)/k(x)$ con $z^2 \in k(x)$; se invece $n > 2$ $k(x)$ contiene tutte le radici dell'unità, quindi per la teoria di Kummer $K^G = k(x)(f^{1/n})$ con $f = f(x) \in k(x)$. Possiamo supporre che sia $f(x) \in k[x]$ con nessun fattore irriducibile di molteplicità $\geq n$.

Dato che l'estensione K/k è regolare abbiamo $N := \overline{\mathbb{Q}}(x)(f^{1/n}) = L^G$. In entrambi i casi possibili almeno una classe di coniugio di $\mathbf{C}$ è contenuta in G (per $n = 2$ basta ricordare che $\sigma_1\sigma_2\sigma_3 = e$), quindi l'estensione $N/\overline{\mathbb{Q}}(x)$ è ramificata solo in $\{0, \infty\}$. Dall'equazione

$$y^n = f(x) = \prod_i (x - \alpha_i)^{m_i}$$

ricaviamo che per $n \geq 2$ vi può essere ramificazione solo in $\{0, \infty\}$ solo nel caso $f(x) = cx^m$; inoltre poiché il grado è proprio n, m deve essere coprimo con n. Se quindi fissiamo a, b interi in modo che sia $ma + nb = 1$, abbiamo che $z := x^b(f^{1/n})^a$ genera K^G su $k(x)$ con $z^n = c^a x \in k(x)$.

A questo punto basta osservare che ponendo $F := k(x)$ otteniamo una GAL-realizzazione, in quanto $\mathrm{Gal}(k(x)/F)$ permuta gli ζz, lasciando quindi invariato il k-spazio vettoriale generato da z. □

Capitolo 4

Esempi e algoritmi

4.1 Costante di struttura

La proprietà di rigidità $l(\mathbf{C}) = 1$ può essere verificata computazionalmente usando l'approccio di forza bruta, ossia verificando manualmente che effettivamente ogni sistema di s generatori di $\mathbf{C}$ è coniugato agli altri. Tale sistema è però palesemente inefficiente. Esiste invece un modo per verificare la rigidità basato sui caratteri irriducibili del gruppo.

Sia $\tilde{\Sigma}(\mathbf{C}) \supset \Sigma(\mathbf{C})$

$$\tilde{\Sigma}(\mathbf{C}) := \{\boldsymbol{\sigma} \in G^s \mid \sigma_i \in C_i, \sigma_1 \cdots \sigma_s = e\}$$

ossia trascuriamo l'ipotesi che i σ_i generino il gruppo G.

Definizione 4.1. Si chiama *costante normalizzata di struttura* di $\mathbf{C} \in \mathrm{Cl}(G)^s$ di un gruppo finito G la quantità

$$n(\mathbf{C}) := \frac{|\tilde{\Sigma}(\mathbf{C})|}{|\operatorname{Inn}(G)|}$$

Proposizione 4.2. *Dato un gruppo finito G ed un vettore di classi $\mathbf{C} \in \mathrm{Cl}(G)^s$ vale*

$$n(\mathbf{C}) = \sum_{[\boldsymbol{\sigma}] \in \tilde{\Sigma}(\mathbf{C})/\operatorname{Inn}(G)} \frac{|Z(G)|}{|\mathcal{C}_G(\langle \sigma_1, \ldots, \sigma_s \rangle)|}.$$

Dimostrazione. Basta applicare l'equazione delle classi per l'azione di $\operatorname{Inn}(G)$

$$\begin{aligned} |\tilde{\Sigma}(\mathbf{C})| &= \sum_{[\boldsymbol{\sigma}] \in \tilde{\Sigma}(\mathbf{C})/\operatorname{Inn}(G)} \frac{|G|}{\operatorname{Stab}_G(\boldsymbol{\sigma})} \\ &= \sum_{[\boldsymbol{\sigma}] \in \tilde{\Sigma}(\mathbf{C})/\operatorname{Inn}(G)} \frac{|G|}{\mathcal{C}_G(\langle \sigma_1, \ldots, \sigma_s \rangle)}. \end{aligned}$$

Ricordando che $|G|/|\operatorname{Inn}(G)| = |Z(G)|$ otteniamo la tesi. □

Teorema 4.3. *Sia* $\mathbf{C} = (C_1, \dots, C_s) \in \mathrm{Cl}(G)^s$ *un vettore di classi di un gruppo finito* G *con* $s \geq 2$*. Allora*

$$n(\mathbf{C}) = |Z(G)| \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{s-2}}{\chi(1)^{s-2}} \prod_{i=1}^{s} \frac{\chi(\sigma_i)}{|\mathcal{C}_G(\sigma_i)|}, \quad \sigma_i \in C_i.$$

Dimostrazione. Per ogni $\chi \in \mathrm{Irr}(G)$ sia $R_\chi : G \to \mathrm{GL}_n(\mathbb{C})$ la corrispondente rappresentazione irriducibile. La funzione lineare

$$\frac{1}{|G|} \sum_{\rho \in G} R_\chi(\sigma^\rho)$$

è G-invariante, quindi per il lemma di Schur è un multiplo dell'identità; è in particolare $\chi(\sigma)/\chi(1)\dot{I}_n$. Quindi per qualsiasi scelta di $\sigma, \tau \in G$ abbiamo

$$\frac{1}{|G|} \sum \rho \in GR(\sigma^\rho \tau) = \frac{\chi(\sigma)}{\chi(1)} R(\tau).$$

Applicando la formula ripetutamente otteniamo

$$\frac{1}{|G|^s} \sum \boldsymbol{\rho} \in G^s R(\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s} \tau) = \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^s} R(\tau).$$

Sostituiamo $\tau = e$ e calcoliamo la traccia:

$$\frac{1}{|G|^s} \sum \boldsymbol{\rho} \in G^s \chi(\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s}) = \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-1}}.$$

Scriviamo ora

$$\epsilon := \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi.$$

La funzione ϵ è il carattere (a meno di un fattore $|G|$) della rappresentazione regolare, quindi vale 1 su e e 0 sul resto. Possiamo allora scrivere

$$m(\mathbf{C}) := \sum_{\rho \in G^s} \epsilon(\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s}) = |G|^{s-1} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-2}}.$$

La funzione $m(\mathbf{C})$ conta il numero di soluzioni $\rho \in G^s$ per cui $\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s} = e$. Possiamo allora scrivere

$$n(\mathbf{C}) = \frac{m(\mathbf{C})}{|\operatorname{Inn}(G)|} \prod_{i=1}^{s} |\operatorname{Stab}_G(\sigma_i)|^{-1} = \frac{m(\mathbf{C})}{|\operatorname{Inn}(G)|} \prod_{i=1}^{s} |\mathcal{C}_G(\sigma_i)|^{-1}.$$

Infine, basta sostituire il valore di $m(\mathbf{C})$ per ricavare la tesi. □

Corollario 4.4. *Un vettore di classi* $\mathbf{C} \in \mathrm{Cl}(G)^s$ *di un gruppo finito* G *è rigido se*

(a) $G = \langle \sigma_1, \dots, \sigma_s \rangle$ *per qualche* $\sigma_i \in C_i$ *con* $\sigma_1 \cdots \sigma_s = e$*,*

(b)

$$\frac{|G|^{s-2}|Z(G)|}{|\mathcal{C}_G(\sigma_1)| \cdots |\mathcal{C}_G(\sigma_s)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-2}} = 1.$$

Dimostrazione. La seconda condizione significa $n(\mathbf{C}) = 1$; dato che $l(\mathbf{C}) \leq n(\mathbf{C})$ otteniamo proprio $l(\mathbf{C}) = 1$. □

4.2 Esempi

Per un elenco piuttosto completo delle realizzazioni note costruite tramite criteri di rigidità si veda [5, Ch. 2].

4.2.1 I gruppi S_n e A_n

L'esempio più classico di gruppo realizzabile come gruppo di Galois su $\mathbb{Q}$ è il gruppo simmetrico ed il suo sottogruppo normale A_n. Una semplice dimostrazione si può ottenere semplicemente considerando l'estensione $\mathbb{Q}(t_1, \dots, t_n)/\mathbb{Q}(s_1, \dots, s_n)$, dove gli s_i sono le funzioni simmetriche elementari dei t_i. Il suo gruppo di Galois è evidentemente S_n. Tramite hilbertianità di $\mathbb{Q}$ abbiamo quindi una realizzazione su $\mathbb{Q}$. Vediamo invece ora come sia possibile utilizzare la rigidità.

Lemma 4.5. *Sia $C^{(i)}$ la classe di coniugio degli i-cicli di S_n, $n \geq 3$. Allora le classi $C^{(2)}$, C^{n-1} e $C^{(n)}$ formano una tripla rigida razionale in S_n.*

Dimostrazione. Innanzitutto notiamo che un qualunque $(n-1)$-ciclo, un qualunque n-ciclo ed una trasposizione generano S_n. Infatti due qualsiasi coppie (i, j) e (i', j') possiamo applicare l'n-ciclo per portare i sul punto fisso dell'$(n-1)$-ciclo, poi spostare liberamente j e infine usare l'n-ciclo per portare l'immagine di i su i' e l'immagine di j (scelta opportunamente) su j'; coniugando allora la trasposizione a disposizione è possibile ottenere tutte le trasposizioni, quindi generare tutto S_n.

Prendiamo ora $\sigma_1 = (n-1, n)$, $\sigma_2 = (1, \dots, n-1)$ e $\sigma_3 = (n, n-1, n-2, \dots, 2, 1)$. Vale $\sigma_1 \cdot \sigma_2 \cdot \sigma_3 = e$ e $S_n = \langle \sigma_1, \sigma_2, \sigma_3$. Supponiamo che $\sigma_1' \sigma_2$ è un n-ciclo, con σ_1' trasposizione. σ_1' è necessariamente della forma (j, n). Allora σ_2^{n-1-j} manda j in $n-1$ e fissa n, quindi σ_1' è coniugato a σ_1 tramite una potenza di σ_2.

Allora data una qualsiasi altra scelta di generatori σ_i' delle stesse classi di coniugio dei σ_i, abbiamo che esiste un coniugio τ che manda σ_2' in σ_2; necessariamente allora σ_1^τ ha la proprietà che $\sigma_1^\tau \sigma_2$ è un n-ciclo. In particolare allora $\sigma_1^\tau = \sigma_1^{\sigma_2^k} = \sigma_2^k \sigma_1 \sigma_2^{-k}$. Usando ora come coniugio $\tau' := \sigma_2^{-k} \tau$ otteniamo $\sigma_1'^{\tau'} = \sigma_1$, $\sigma_2'^{\tau'} = \sigma_2$ e di conseguenza $\sigma_3'^{\tau'} = \sigma_3$. Quindi $\Sigma(\mathbf{C})$ ha una sola orbita per l'azione di $\mathrm{Inn}(G)$, ossia $l(\mathbf{C}) = 1$ e il vettore è rigido.

Per ogni $m \nmid n!$ gli i-cicli restano evidentemente i-cicli, quindi anche la condizione di razionalità è soddisfatta da $\mathbf{C}$. □

In questo modo otteniamo

Corollario 4.6. *S_n ha una G-realizzazione su $\mathbb{Q}$ per ogni n.*

Dimostrazione. Il caso $n \geq 3$ si ottiene dal lemma 4.5 unito al teorema 2.19 e il fatto che $Z(S_n) = \{e\}$. Il caso $n = 2$ si ricava immediatamente dal fatto che $S_2 \cong \mathbb{Z}_2$ si realizza come $\mathbb{Q}(y)/\mathbb{Q}(x)$ dove $y^2 = x$. □

Nel caso in cui $n \neq 6$ abbiamo anche $\mathrm{Aut}(A_n) \cong S_n$ e $\mathrm{Aut}(S_n) = S_n$, mentre vale sempre $[S_n : A_n] = 2$; ricaviamo quindi dalla proposizione 3.20 il seguente corollario.

Corollario 4.7. *Per $n \neq 6$ i gruppi A_n e S_n hanno GAL-realizzazione su $\mathbb{Q}$, quindi su tutti i campi di caratteristica 0.*

Dalla dimostrazione della proposizione 3.20 notiamo che comunque anche A_6 ha una G-realizzazione su $\mathbb{Q}$; non otteniamo però una GA-realizzazione, quindi nemmeno una GAL-realizzazione.

4.2.2 Il gruppo $\mathrm{PSL}_2(p)$

Un esempio relativamente semplice di applicazione del criterio di rigidità si può costruire su una sottofamiglia dei gruppi semplici $A_n(q)$; ci concentreremo ora sul caso in cui q è un primo dispari e $n = 2$, ovvero su $\mathrm{PSL}_2(p) \cong \mathrm{SL}_2(p)/\{\pm 1\}$.

Lemma 4.8. *Il gruppo $\mathrm{SL}_2(p)$, e quindi anche $\mathrm{PSL}_2(p)$, è generato da*

$$U_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U_1^T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Dimostrazione. Notiamo che

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} U_1^k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+ka \\ c & d+ka \end{pmatrix},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (U_1^T)^k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} = \begin{pmatrix} a+kb & b \\ c+kd & d \end{pmatrix}.$$

Moltiplicando a destra per U_1^T possiamo assicurarci che il coefficiente a diventi non nullo; usando invece U_1 possiamo assicurarci che anche il coefficiente in b non lo sia, ed utilizzando di nuovo U_1^T ridurci al caso $a = 1$. A questo punto possiamo tramite moltiplicazione per U_1 trasformare il coefficiente b in 0. Per ipotesi sul determinante otteniamo allora $d = 1$. La matrice che rimane è allora una potenza di U_1^T. □

Lemma 4.9. *Sia U una matrice non triangolare superiore in $\mathrm{SL}_2(p)$ con traccia 2. Allora U è coniugata ad una potenza di U_1^T tramite una potenza di U_1.*

Dimostrazione. Scrivendo $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ possiamo calcolare:

$$U_1^k A U_1^{-k} = \begin{pmatrix} a+kc & * \\ c & * \end{pmatrix}.$$

Per ipotesi $c \neq 0$, quindi scegliendo $k = (1-a)c^{-1}$ e ricordando l'ipotesi su traccia e determinante otteniamo

$$U_1^k A U_1^{-k} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = (U_1^T)^c.$$

□

Lemma 4.10. *Le matrici di $\mathrm{PSL}_2(p) \setminus \{e\}$ di traccia ± 2 appartengono ad esattamente due classi di coniugio C_1 e C_2 rappresentate da $\pm U_1$ e $\pm U_1^T$. Una matrice $\pm \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$*

(oppure $\pm\begin{pmatrix}1 & 0\\ v & 1\end{pmatrix}$*) è coniugata a* $\pm U_1$ *se e soltanto* u *(rispettivamente* $-v$*) è un quadrato in* $\mathbb{F}_p$*.*

Dimostrazione. Se $\pm U \in \mathrm{PSL}_2(p)$ è triangolare superiore ha un rappresentante in $\mathrm{SL}_2(p)$ della forma $\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$.

Sia $U \in \mathrm{SL}_2(p)$ di traccia 2 rappresentante di $\pm U \in \mathrm{PSL}_2(p)$ che non sia in forma triangolare superiore. Il lemma 4.9 ci garantisce che U è coniugata ad una potenza di U_1^T della forma $\begin{pmatrix}1 & 0\\ v & 1\end{pmatrix}$. Sfruttiamo allora l'uguaglianza

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ v & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & -v\\ 0 & 1\end{pmatrix}$$

per ridurci al caso triangolare superiore. Supponiamo ora che $\pm B$ coniughi $\pm U_1$ in $\pm\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$; B deve necessariamente essere triangolare superiore, poiché il sottospazio generato dal vettore $\begin{pmatrix}1\\ 0\end{pmatrix}$ deve restare fisso. Quindi

$$\pm\begin{pmatrix}w & *\\ 0 & w^{-1}\end{pmatrix} U_1 \begin{pmatrix}w & *\\ 0 & w^{-1}\end{pmatrix}^{-1} = \pm\begin{pmatrix}1 & w^2\\ 0 & 1\end{pmatrix}.$$

La soluzione si ha solamente se u $(-v)$ è un quadrato. Se non è questo il caso possiamo invertire la situazione

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ -u & 1\end{pmatrix}$$

e ripetere l'identico ragionamento con U_1^T, sapendo questa volta che $-u$ e v sono quadrati. □

Lemma 4.11. *Sia* $\tau \neq 1, 2$*. Sia* $C(\tau)$ *la classe di coniugio in* $\mathrm{PSL}_2(p)$ *di* $\pm\begin{pmatrix}\tau-1 & 1\\ \tau-2 & 1\end{pmatrix}^{-1}$*. Se* $2-\tau$ *non è un quadrato (rispettivamente, è un quadrato) in* $\mathbb{F}_p$ *allora la terna* $C_1, C_2, C(\tau)$ *(rispettivamente,* $C_1, C_1, C(\tau)$*) è rigida.*

Dimostrazione. La matrice $\pm\begin{pmatrix}\tau-1 & 1\\ \tau-2 & 1\end{pmatrix}$ appartiene a C_2 (risp., C_1) se $(2-\tau)$ non è un quadrato (risp., è un quadrato) per il lemma 4.10. Scrivendo

$$\pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & 0\\ \tau-2 & 1\end{pmatrix}^{-1} = \pm\begin{pmatrix}\tau-1 & 1\\ \tau-2 & 1\end{pmatrix}$$

mostra che esistono $\sigma_1 \in C_1$, $\sigma_2 \in C_2$ e $\sigma_3 \in C_3$ per cui $\sigma_1\sigma_2\sigma_3 = e$ (risp., $\sigma_2 \in C_1$). Sappiamo dal lemma 4.8 che σ_1 e σ_2 generano $\mathrm{PSL}_2(p)$, in quanto $\sigma_2 = (U_1^T)^k$ con $k \neq 0$.

Supponiamo ora di avere un'altra terna di generatori $\sigma_1', \sigma_2', \sigma_3'$. Tramite un primo coniugio possiamo supporre che $\sigma_1' = \sigma_1$. Ci basta allora verificare che $\sigma_2' \in C_2$ (risp., C_1) è coniugato a σ_2 tramite un elemento che commuta con

σ_1. Dato che σ_1 e σ_2' generano tutto il gruppo certamente σ_2' non è triangolare superiore; per il lemma 4.9 è allora coniugato ad una matrice della forma $\pm\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}$ tramite un elemento che commuta con σ_1.

Considerando ora che la traccia è una funzione costante sulle classi di coniugio, abbiamo che $\sigma_1\sigma_2'$ ha la stessa traccia di $\sigma_1\sigma_2$ ed è quindi τ. Essendo allora anche la traccia di $\sigma_1\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}$, vale $c = \tau - 2$. Il lemma 4.10 ci fornisce quindi il risultato. □

Lemma 4.12. *Sia $\mathbf{C}(\tau)$ il vettore di classi costruito nel lemma 4.11 e V il suo gruppo completo di simmetria. Se $p \not\equiv \pm 1 \pmod{24}$ e $p > 3$, allora esiste un τ per cui $\mathbf{C}(\tau)$ è V-simmetrico.*

Dimostrazione. Scegliamo τ in modo che $(2-\tau)$ non sia un quadrato (esiste poiché $p > 3$). In questo caso $\mathbf{C}(\tau)$ è la terna $(C_1, C_2, C(\tau))$; abbiamo che $C_1^m = C_1$ quando $m \in \mathbb{F}_p^*$ è un quadrato in $\mathbb{F}_p$ e $C_1^m = C_2$ quando non lo è per il lemma 4.10. La terna $\mathbf{C}$ è allora V-simmetrica solamente quando $C(\tau)^m = C(\tau)$, poiché se $C(\tau)^k = C_i$ avremmo anche $C(\tau) = C_i^{k'} = C_j$ con $i, j \in \{1, 2\}$, mentre la traccia degli elementi di $C(\tau)$ è $\tau \neq \pm 2$.

Se 2 (risp., 3) è un non quadrato in $\mathbb{F}_p$, possiamo porre $\tau = 0$ (risp., $\tau = -1$). Siano $A_2 := \begin{pmatrix}-1 & 1\\ -2 & 1\end{pmatrix}$ e $A_3 := \begin{pmatrix}-2 & -3\\ -1 & 1\end{pmatrix}$. Notiamo che $A_2^2 = -e$, quindi in $\mathrm{PSL}_2(p)$ $C(2)$ è una classe razionale, mentre da $A_3^3 = e$ deduciamo che A_3 e A_3^2 soddisfano lo stesso polinomio caratteristico

$$X^2 - X + 1.$$

Tale polinomio ha due radici distinte in $\mathbb{F}_p(\sqrt{3})$, quindi A_3 e A_3^2 sono coniugate con coefficienti in $\mathbb{F}_p(\sqrt{3})$. Tale coniugio si riporta (come nel caso della forma di Jordan reale) in $\mathrm{SL}_2(p)$, quindi anche in $\mathrm{PSL}_2(p)$.

Ora 2 è non quadrato modulo p se e soltanto se $p \not\equiv \pm 1 \pmod{8}$, mentre 3 non è un quadrato modulo p se e soltanto se $p \not\equiv 1 \pmod{3}$. Quindi se $p \not\equiv \pm 1 \pmod{24}$ abbiamo che per almeno una scelta $\tau = 0, -1$ si ha $\mathbf{C}^V = \mathbf{C}^*$, ovvero $\mathbf{C}$ è V-simmetrico. □

Teorema 4.13. *Il gruppo $\mathrm{PSL}_2(p)$ occorre regolarmente su $\mathbb{Q}$ per ogni primo $p \not\equiv \pm 1 \pmod{24}$.*

Dimostrazione. Se $p > 3$ il lemma 4.12 esiste una terna $\mathbf{C}$ razionale e V-simmetrica, con $V = \mathrm{Sym}(\mathbf{C})$; per il teorema 2.24 esiste una G-realizzazione su $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$, quindi $\mathrm{PSL}_2(p)$ occorre regolarmente su $\mathbb{Q}$.

Per i casi restanti notiamo che $\mathrm{PSL}_2(2) \cong S_3$, poiché in tal caso si tratta di tutte le permutazioni dei tre punti di $\mathbb{P}^1(\mathbb{F}_2)$, mentre $\mathrm{PSL}_2(3) \cong A_4$, poiché sono l'unico sottogruppo delle permutazioni dei quattro punti di $\mathbb{P}^1(\mathbb{F}_3)$ di indice 2 (il determinante delle matrici invertibili può avere 2 valori possibili ed è surgettivo). Entrambi i gruppi hanno una G-realizzazione per il corollario 4.7. □

Teorema 4.14. *Il gruppo* $\mathrm{PSL}_2(p)$ *occorre regolarmente su* $\mathbb{Q}^{ab}$ *per ogni primo* p.

Dimostrazione. Per tutti i casi non compresi nel teorema 4.13 vale comunque che **C** è una terna rigida, quindi per il teorema 2.24 esistono G-realizzazioni su estensioni abeliane di $\mathbb{Q}$ finite; in particolare allora esistono G-realizzazioni su $\mathbb{Q}^{ab}$. □

4.3 Algoritmi

Nel lavoro [4] sono presentate brevemente le varianti algoritmiche delle tecniche descritte nel capitolo 3, e sono esplicitati i risultati con i quali si dimostra che tutti i gruppi transitivi di ordine fino a 15 si realizzano su $\mathbb{Q}$. Ne accenniamo qui rapidamente le idee fondamentali basate tutte sulla tecnica del risolvente, che può essere usata efficacemente sia per i calcoli che vedremo ora sia per risolvere il problema diretto, ovvero ricostruire il gruppo di Galois a partire da un polinomio. Di fatto la strategia del cosiddetto metodo Stauduhar [7] è sostanzialmente equivalente all'argoritmo del campo fisso che vedremo fra breve. Lavoriamo assumendo che siano dati un polinomio f monico irriducibile a coefficienti in $\mathbb{Z}$, l'insieme $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ delle sue radici e G il gruppo di Galois di f comprensivo della sua azione di permutazione su Ω.

4.3.1 Algoritmo del campo fisso

Supponiamo di avere un gruppo di permutazione $\tilde{G}$ ed un epimorfismo $\phi : G \to \tilde{G}$. Sia $\tilde{H}$ lo stabilizzatore di un punto in $\tilde{G}$. Chiamiamo allora H la controimmagine $\phi^{-1}(\tilde{H})$; il gruppo G agirà sulle classi laterali G/H come $\tilde{G}$. Cerchiamo di calcolare un polinomio g che sia il polinomio minimo di un elemento del campo $\mathrm{Fix}(H)$. Facciamo cadere, in questo algoritmo, l'ipotesi che f sia irriducibile, ma assumeremo solo che sia separabile (condizione che è facile imporre sostituendo f con $f/\gcd(f, f')$); tra le sue possibili applicazioni ci sarà, infatti, la costruzione di un polinomio $\tilde{f}$ irriducibile che ha lo stesso campo di spezzamento di f.

Definizione 4.15. Sia G un gruppo di permutazione che agisce su un insieme $\{\alpha_1, \ldots, \alpha_n\}$ e H un suo sottogruppo. Ponendo $x_i := x_{\alpha_i}$, con x_i variabili indipendenti, diciamo che un polinomio $F \in \mathbb{Z}[x_1, \ldots, x_n]$ è *H-invariante relativamente a G* se

(a) $F^\sigma = F$ per ogni $\sigma \in H$,

(b) $F^\sigma \neq F$ per ogni $\sigma \in G \setminus H$

dove con F^σ si intende l'azione data da $x_i^\sigma = x_{\alpha_i}^\sigma = x_{\sigma(\alpha_i)}$.

In questo caso si chiama *risolvente* il polinomio

$$R_{G,H,F} := \prod_{\sigma \in G//H} (X - F^\sigma) \in \mathbb{Z}[x_1, \ldots, x_n, X]$$

dove $G//H$ è un sistema di rappresentanti delle classi laterali G/H.

Osservazione 4.16. Per ogni $H < G$ esiste sempre un polinomio H-invariante relativamente a G. Basta prendere

$$F(x_1, \dots, x_n) := \sum_{\sigma \in H} (x_1^1 x_2^2 \cdots x_n^n)^\sigma.$$

Un modo alternativo più efficiente per costruire un polinomio H-invariante relativamente a G è il seguente:

1. Porre $d := 1$.
2. Calcolare tutti i polinomi omogenei H-invarianti di grado d.
3. Controllare che siano relativi a G, ossia che non restino fissati da nessun $\sigma \in G \setminus H$.
4. Se ve ne sono di relativi a G, restituirne uno.
5. Porre $d := d = 1$ e tornare al passo 2.

Un polinomio H-invariante relativo a G ha l'interessante proprietà per cui $F(\alpha_1, \dots, \alpha_n) \in \mathrm{Fix}(H)$, mentre il polinomio $R_{G,H,F}$ specializzato è il suo polinomio caratteristico su $\mathbb{Q}$. Allora $R_{G,H,F}$ è potenza di un polinomio irriducibile, e nel caso in cui sia irriducibile si ha proprio $\mathrm{Gal}(R_{G,H,F}) \cong \tilde{G}$. Per ottenere che $R_{G,H,F}$ specializzato sia irriducibile dobbiamo cambiare il polinomio f, a patto di conservarne il campo di spezzamento.

Definizione 4.17. Sia $f(x) \in k(x)$ un polinomio e siano $\alpha_1, \dots, \alpha_n$ le sue radici. Un polinomio $h \in k(t)$ si dice *trasformazione di Tschirnhausen* per f se il campo di spezzamento del polinomio ${}^h f(x) := \prod(x - h(\alpha_i))$ è lo stesso di f.

Osservazione 4.18. Data un polinomio $h(x) \in k(x)$, se il polinomio ${}^h f(x)$ è separabile allora h è una trasformazione di Tschirnhausen. Se infatti $g(x) = \prod_\sigma (x - \sigma(\alpha))$ è un fattore irriducibile di f, avremo che ${}^h g(x) = \prod_\sigma (x - \sigma(h(\alpha)))$ ha radici distinte. In particolare allora il campo di spezzamento di ${}^h g$ non è lasciato fisso da nessun automorfismo non banale del campo di g, quindi i due campi sono uguali.

Possiamo allora applicare una trasformata di Tschirnhausen ad f. Usiamo l'idea di [3] per verificare che è effettivamente calcolabile una trasformata che renda $R_{G,H,F}$ irriducibile.

Lemma 4.19. *Esiste un insieme finito $T \subset k[x]$, dipendente da $R_{G,H,F}$ e da f ed effettivamente calcolabile, tale per cui esista una trasformazione di Tschirnhausen tale per cui ${}^h f$ e $R_{G,H,F}(h(\alpha_1), \dots, h(\alpha_n))$ sono separabili.*

Dimostrazione. Sia $\hat{f}(x_1, \dots, x_n, x) = \prod_i (x - x_i)$. Sia d un intero maggiore del grado totale del discriminante

$$D^2(x_1, \dots, x_n) := D_x^2(\hat{f} \cdot R_{G,H,F}) = \pm \prod_{i \neq j} (x_i - x_j) \prod_{\sigma \neq \tau} (F^\sigma - F^\tau) \in k(x_1, \dots, x_n).$$

Poniamo $y_i := \sum_{j=0}^{n-1} \alpha_i^j z_j$, con z_j nuove variabili. Poiché per ipotesi di separabilità di f le radici α_i sono tutte distinte, le variabili y_i sono algebricamente

indipendenti quanto le z_j (la matrice di trasformazione da z_i a y_i è infatti di Vandermonde sugli α_i, quindi invertibile). In particolare allora il polinomio $D^2(y_1, \ldots, y_n) \neq 0$ ed ha grado massimo rispetto ad ogni y_i minore di d. In particolare allora se fissiamo un insieme $U \subset k$ di cardinalità d, esisterà una scelta di specializzazioni $y_i \mapsto u_i \in U$ tale per cui $D^2(u_1, \ldots, u_n) \neq 0$. Il polinomio $h(x) = \sum u_i x^i$ è allora la trasformata richiesta ed appartiene a $T = \{u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} + x^n \mid u_i \in U\}$. □

Riepilogando:

1. Calcolare un polinomio F che sia H-invariante relativo a G.
2. Generare un insieme $T(\alpha_1, \ldots, \alpha_n)$ di trasformazioni di Tschirnhausen come nel lemma 4.19.
3. Calcolare $R_{G,H,F}(\alpha_1, \ldots, \alpha_n)$.
4. Se $\gcd(R_{G,H,F}(\alpha_1, \ldots, \alpha_n), R'_{G,H,F}(\alpha_1, \ldots, \alpha_n)) = 1$ restituire $R_{G,H,F}(\alpha_1, \ldots, \alpha_n)$.
5. Applicare una trasformazione di T all'insieme di radici $\{\alpha_1, \ldots, \alpha_n\}$ e tornare al passo 3.

4.3.2 Prodotto diretto

Supponiamo ora di avere due polinomi irriducibili $f_1, f_2 \in \mathbb{Z}[x]$ tali per cui $G_1 = \mathrm{Gal}(f_1)$ e $G_2 = \mathrm{Gal}(f_2)$. Siano N_1 e N_2 i relativi campi di spezzamento e supponiamo che sia $N_1 \cap N_2 = \mathbb{Q}$. Si consideri come sempre già descritta l'azione di G_1 e G_2 sui rispettivi insiemi di radici che chiameremo $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_m\}$.

1. Porre $\tilde{f} := f_1 f_2$.
2. Porre $\tilde{G}$ il prodotto diretto di G_1 e G_2 con l'azione indotta sull'insieme $\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$.
3. Calcolare il polinomio f restituito dall'algoritmo del campo fisso applicato a $\tilde{f}$ e all'epimorfismo identico da $\tilde{G}$ su G.
4. Restituire f.

4.3.3 Prodotto a ghirlanda

Sia G dato come i gruppi precedenti e H un gruppo di Galois su $\mathbb{Q}(t)$, realizzato regolarmente con un polinomio $g(t, x) \in \mathbb{Z}[t, x]$.

1. Sia $K := \mathbb{Q}(\alpha)$, con α zero di f.
2. Sia γ un intero algebrico scelto casualmente in K.
3. Porre $h := N(g(\gamma, x))$, con N norma da K a $\mathbb{Q}$ estesa a $K(x)$ ponendo $N(x) = x$.
4. Se h è riducibile tornare al passo 2.

5. Se $\mathrm{Gal}(h) \cong H \wr G$ restituire h, altrimenti tornare al passo 2.

I possibili γ sono infiniti per la proprietà di hilbertianità.

Appendice A

Metodi non standard

L'utilizzo dei modelli non standard consente di dare uno sguardo diverso alla proprietà di hilbertianità, fornendo caratterizzazioni di natura algebrica assai diverse dalle proprietà studiate nella sezione 1.1. La dimostrazione originale del teorema 1.14, pubblicata in [10] con riferimenti a [6], fa proprio uso di questi strumenti, dai quali si ricava anche l'hilbertianità di tutti i campi con formula del prodotto.

A.1 Ingrandimenti

Per una presentazione tradizionale della teoria dei modelli non standard si veda [8]. Daremo ora le definizioni ed enunceremo i fatti fondamentali di cui faremo uso in seguito.

Dato un insieme X qualsiasi, i cui singoli oggetti sono considerati privati della struttura insiemistica, costruiamo su di esso la successione di insiemi

$$\begin{aligned} X_0 &:= X \\ X_{n+1} &:= \mathscr{P}\left(\bigcup_{k=0}^{n} X_k\right) \quad n \in \mathbb{N} \end{aligned}$$

e poniamo $\mathscr{X} := \cup_{k=0}^{\infty} X_k$.

Definizione A.1. L'insieme $\mathscr{X}$ si dice *sovrastruttura* di X. Gli elementi di X vengono detti *atomi*, mentre i restanti vengono denominati *entità*.

È una verifica semplice controllare, a patto di trascurare l'eventuale struttura insiemistica sugli elementi di X, che la sovrastruttura è chiusa per le comuni operazioni di teoria degli insiemi.

Proposizione A.2. *(a)* $\emptyset \in \mathscr{X}$.

(b) Se y è un'entità, ogni $x \in y$ appartiene a $\mathscr{X}$.

(c) Se y è un'entità, ogni $x \subset y$ è un'entità.

(d) Se x è un'entità, $\mathscr{P}(x)$ è un'entità.

(e) Ogni sottoinsieme x finito di $\mathscr{X}$ è un'entità.

(f) Se x è un'entità, $\bigcup x = \bigcup_{y \in x} y$ è un'entità.

(g) Se x e y sono entità, la coppia (x, y) è un'entità.

(h) Se l'assioma della scelta è vero nella teoria insiemistica in cui si costruisce $\mathscr{X}$, allora è vera anche la sua formulazione in $\mathscr{X}$.

Definizione A.3. Una mappa $* : \mathscr{X} \to {}^*\mathscr{X}$ si dice *omomorfismo di sovrastrutture* se

(a) Per ogni entità x vale $\{{}^*y \mid y \in x\} \subset {}^*x\}$ e si ha inclusione stretta per ogni x infinito.

(b) ${}^*X$ è l'insieme degli atomi di ${}^*\mathscr{X}$.

(c) Se $x \in y$ per due entità, ${}^*x \in {}^*y$.

(d) Preserva la relazione di uguaglianza: ${}^*\{(x, x) \mid x \in X\} = \{(y, y) \mid y \in {}^*X\}$.

(e) Se $y = \{x_1, \ldots, x_n\}$ è un insieme finito, ${}^*y = \{{}^*x_1, \ldots, {}^*x_n\}$.

(f) ${}^*\emptyset = \emptyset$.

(g) ${}^*(x \cap y) = {}^*x \cap {}^*y$, ${}^*(x \cup y) = {}^*x \cap {}^*y$.

(h) Preserva domini e immagini delle relazioni.

(i) ${}^*\{(x, y) \mid x \in y \in A\} = \{(z, w) \mid z \in w \in {}^*A\}$.

Teorema A.4 (Trasferimento)**.** *Per ogni formula φ del prim'ordine nel linguaggio della teoria degli insiemi con parametri in $\mathscr{X}$*

$$\mathscr{X} \models \varphi \iff {}^*\mathscr{X} \models {}^*\varphi$$

dove con ${}^*\varphi$ si intende la formula φ nella quale i parametri sono stati trasformati secondo $*$.

Definizione A.5. Una relazione binaria $R(x, y)$ su X è detta *finitamente soddisfacibile* se per ogni scelta $x_i \in X$, con $i = 0, \ldots, n$, esiste un $\omega \in X$ per il quale $R(x_i, \omega)$ è verificato per tutti gli i.

Definizione A.6. Un omomorfismo di sovrastrutture $* : \mathscr{X} \to {}^*\mathscr{X}$ si dice *ingrandimento* se ogni relazione binaria R finitamente soddisfacibile ha una *soluzione universale* $\omega \in {}^*X$ per la quale $R(x, \omega)$ vale per ogni $x \in X$.

Teorema A.7. *Ogni struttura $\mathscr{X}$ ha un ingrandimento ${}^*\mathscr{X}$.*

Identificheremo d'ora in poi, parlando di ingrandimenti, la sovrastruttura $\mathscr{X}$ con la sua immagine in ${}^*\mathscr{X}$.

Lemma A.8. *Per un ingrandimento $*$ si ha ${}^*A = A$ se e soltanto se A è finito.*

Dimostrazione. Se A è finito ${}^*A = A$ per definizione di omomorfismo di sovrastrutture.

Se invece A è infinito, la relazione $\neq$ ristretta all'insieme A è finitamente soddisfacibile, quindi in ${}^*A$ possiede una soluzione universale ω. Pertanto $\omega \in {}^*A \setminus A$, quindi ${}^*A \neq A$. □

A.2 Hilbertianità

Sia ora k un campo di caratteristica 0 e $*$ un ingrandimento fissato. ${}^*k$ è naturalmente un'estensione di campo di k, identificando k con l'immagine tramite $*$ dei suoi elementi.

Proposizione A.9. *k è algebricamente chiuso in ${}^*k$.*

Dimostrazione. Fissati $a_0, \dots, a_n \in k$ coefficienti di un polinomio privo di radici in k abbiamo per trasferimento che

$$\exists x(a_0 + \cdots + a_n x^n = 0)$$

è falsa in ${}^*k$, quindi in particolare il polinomio continua a non avere radici nemmeno in ${}^*k$. □

Abbiamo quindi che ogni elemento $t \in {}^*k \setminus k$ è trascendente su k. Possiamo allora riformulare la proprietà di Hilbert:

Proposizione A.10. *k è hilbertiano se e soltanto se esiste un $t \in {}^*k \setminus k$ per cui $k(t)$ è algebricamente chiuso in ${}^*k$.*

Dimostrazione. Sia $t \in {}^*k \setminus k$ un elemento tale per cui $k(t)$ sia algebricamente chiuso in ${}^*k$. Siano $f_i(X, T)$ polinomi irriducibili in T, con $i = 1, \dots, s$; per trascendenza di t, anche i polinomi $f_i(X, t)$ sono tutti irriducibili. Fissati quindi $t_1, \dots, t_n$ un numero finito arbitrario di elementi di k è verificata la formula

$$\exists v : \forall 1 \leq i \leq s \ f_i(X, v) \text{ è irriducibile}, v \neq t_1, \dots, t_n.$$

Per trasferimento questa formula è vera anche in k, quindi esistono infiniti $v \in k$ per i quali gli $f_i(X, v)$ sono irriducibili, ossia k è hilbertiano.

Se viceversa k è hilbertiano, la relazione

$$R((x, f), v) \leftrightarrow f(X, v) \text{ è irriducibile}, v \neq x$$

ristretta ai polinomi $f \in k(X)[T]$ irriducibili in T è finitamente soddisfacibile, quindi ha una soluzione universale t per la quale $f(X, t)$ è irriducibile in ${}^*k(X)[T]$ per tutti i polinomi $f(X, T)$ irriducibili; inoltre vale necessariamente $t \in {}^*k \setminus k$. Allora $k(t)$ è algebricamente chiuso in ${}^*k$. □

Proposizione A.11. *k è hilbertiano se e soltanto se esiste un sottocampo $k \subset l \subset {}^*k$ hilbertiano e algebricamente chiuso in ${}^*k$.*

Dimostrazione. Se k è hilbertiano è sufficiente scegliere $l = k$.

Sia invece l un sottocampo hilbertiano algebricamente chiuso in ${}^*k$. Se prendiamo un'ulteriore ingrandimento $+$ abbiamo che esiste un $t \in {}^+l \setminus l$ per il quale $l(t)$ è algebricamente chiuso in ${}^+l$. Per trasferimento ${}^+l$ è algebricamente chiuso in ${}^+({}^*k)$, quindi vale $\overline{k(t)} \cap {}^+({}^*k) = \overline{k(t)} \cap {}^+l = \overline{k(t)} \cap \overline{l(t)} \cap {}^+l = k(t)$ per trascendenza di t su l.

Basta ora osservare che $+ \circ *$ è un ingrandimento di k, quindi k è hilbertiano. □

Definiamo ora il campo l_t come la chiusura algebrica di $k(t)$ in ${}^*k$, al variare di $t \in {}^*k \setminus k$.

Lemma A.12. *Siano L_1 ed L_2 due estensioni finite di un campo K di caratteristica 0 e sia L il loro composto. Dato un posto $\mathfrak{P}$ in L ramificato su K, se gli indici di ramificazione della restrizione a L_1 e L_2 coincidono allora L/L_1 e L/L_2 sono estensioni non ramificate in $\mathfrak{P}$.*

Dimostrazione. Chiamiamo $\mathfrak{P}_1$ e $\mathfrak{P}_2$ le restrizioni di $\mathfrak{P}$ su L_1 e L_2 rispettivamente. Sia invece $\mathfrak{P}'$ la restrizione a K. Il gruppo di inerzia di $\mathfrak{P}$ su $\mathfrak{P}'$ è ciclico di ordine $e(\mathfrak{P}|\mathfrak{P}')$; sia σ un suo generatore. Se i gruppi di inerzia di $\mathfrak{P}_1$ e $\mathfrak{P}_2$, che sono immagine tramite restrizione di $G_I(\mathfrak{P}|\mathfrak{P}')$, hanno lo stesso ordine, esiste un intero f minimo tale per cui σ^f ha immagine banale se ristretto a L_1 e L_2. Dato però che L è il composto di L_1 e L_2, σ^f è banale su L e quindi $f = e(\mathfrak{P}|\mathfrak{P}')$. In particolare allora la ramificazione non aumenta da L_1 e L_2 a L. □

Proposizione A.13. *k è hilbertiano se e soltanto se esiste un $t \in {}^*k \setminus k$ ed un posto di $\mathbb{P}(k(t)/k)$ che abbia solamente un numero finito di estensioni a l_t.*

Dimostrazione. Ovviamente se k è hilbertiano ricaviamo dalla proposizione A.10 un t tale per cui $k(t) = l_t$. Allora qualunque posto di $\mathbb{P}(k(t)/k)$ ha un'unica estensione in l_t.

Supponiamo invece che k non sia hilbertiano. Esistono allora un numero finito di polinomi $f_1(X,T), \dots, f_n(X,T)$ irriducibili in T di grado maggiore di 0 in T, tali per cui per quasi tutti i valori $t \in k$ almeno un polinomio $f_i(X,t)$ è riducibile. Dato che gli insiemi finiti vengono conservati tramite la mappa $*$, vale allora che per ogni $s \in {}^*k \setminus k$ almeno un polinomio $f_i(X,s)$ è riducibile in ${}^*k$.

Fissato allora un $t \in {}^*k \setminus k$ abbiamo che i polinomi $f_i(X,t)$ sono irriducibili su $k(t)$ per trascendenza di t, mentre almeno uno di essi diventa riducibile in ${}^*k$; quindi, chiamando K il campo di spezzamento degli $f_i(X,t)$ su $k(t)$, abbiamo $K \cap {}^*k \neq k(t)$.

Possiamo dire di più. Prendiamo un posto $\mathfrak{P} \in \mathbb{P}(k(t)/k)$ di grado uno che non sia ramificato in F; chiamiamo i Φ il sottogruppo di $\mathrm{Aut}(k(t)/k)$ che lasciano P fisso. Ogni elemento $\alpha \in \Phi$ si estende ad un automorfismo della chiusura algebrica di $k(t)$, pertanto per ogni estensione $\tilde{\alpha}$ è definito $K^{\tilde{\alpha}}$; essendo K un'estensione normale di $k(t)$, $K^{\tilde{\alpha}}$ non dipende dalla particolare estensione scelta, quindi scriveremo d'ora in poi K^α. Ovviamente F^α sarà il campo di spezzamento dei polinomi $f_i(X,t^\alpha)$. Dato che di nuovo almeno uno degli $f_i(X,t^\alpha)$ diventa riducibile in ${}^*k$, poiché $t^\alpha \notin k$, abbiamo che $K^\alpha \cap {}^*k \neq k(t)$. Definiamo K^Φ come il composto di tutte le estensioni K^α al variare di $\alpha \in \Phi$.

Sia ora D_K l'insieme dei posti di $k(t)$ ramificati in K e D_Φ l'insieme dei posti ramificati in $K^\Phi \cap {}^*k$. Dato che $K^\alpha \cap {}^*k \neq k(t)$ esiste almeno un posto che si ramifica in K^α, $D_K^\alpha \cap D_\Phi \neq \emptyset$ per ogni $\alpha \in \Phi$. L'azione di Φ è però l'azione di $PGL_2(k)$, dunque agisce transitivamente sulle terne di posti di primo grado; in particolare D_Φ deve essere quindi infinito, perché è possibile mandare un posto qualsiasi in un altro lasciando fisso $\mathfrak{P}$. Otteniamo allora $[K^\Phi \cap {}^*k : k(t)] = \infty$.

Osserviamo ora che fissata $\tilde{\mathfrak{P}}$ estensione di Pf in K, il suo campo residuo è un'estensione normale del campo residuo di $\mathfrak{P}$; in particolare allora i campi residui dei $\tilde{\mathfrak{P}}^\alpha$ coincidono tutti, da cui deduciamo che per una qualsiasi estensione $\overline{\mathfrak{P}}$ in K^Φ il campo residuo, essendo il composto dei campi residui delle sottoestensioni che generano K^Φ, ha grado finito. Sommando questo al fatto che $\mathfrak{P}$ resta non ramificato in tutte le estensioni K^α, quindi anche in K^Φ, abbiamo che deve avere infinite estensioni in K^Φ, quindi anche in l_t.

Se il posto $\mathfrak{P}$ non è di grado 1 sappiamo che avrà un parametro locale della forma $u := t^k + a_{k-1} + \cdots + a_0$; considerando allora $k(u)$ e $\mathfrak{P}' \in \mathbb{P}(k(u)/k)$ tale per cui $\mathfrak{P} \mid \mathfrak{P}'$, possiamo ripetere il ragionamento prendendo $\Phi < \mathrm{Aut}(k(u)/k)$ lo stabilizzatore di $\mathfrak{P}'$. Otteniamo di nuovo che $\mathfrak{P}'$ ha infinite estensioni in l_t; sappiamo però che $\mathfrak{P}$ è l'unico posto sopra $\mathfrak{P}'$ dal confronto dei gradi, quindi anche $\mathfrak{P}$ ha infinite estensioni in l_t.

Per concludere, ci basta osservare che nel caso ramificato esistono sempre almeno due posti ramificati, dunque anche $D_K^\alpha \cap D_\Phi \setminus \{\mathfrak{P}\} \neq \emptyset$; inoltre le estensioni K^α hanno tutte lo stesso indice di ramificazione per qualsiasi estensione di $\mathfrak{P}$, quindi per il lemma A.12 il composto K^Φ ha anch'esso indice di ramificazione finito e $\mathfrak{P}$ ha infinite estensioni in l_t. □

A.3 Valori assoluti

Sia S un insieme di valori assoluti k. Consideriamo i suoi elementi in forma logaritmica, ovvero $v(\cdot) = -\log|\cdot|$. Se definiamo

$$\mathcal{O}_v = \{x \in k \mid v(x) \geq 0\}$$

e

$$\mathcal{O}_S = \bigcap_{v \in S} \mathcal{O}_v = \{x \in k \mid v(x) \geq 0 \ \forall v \in S\}$$

otteniamo immediatamente

$${}^*(\mathcal{O}_S) = \{x \in {}^*k \mid v(x) \geq 0 \ \forall v \in {}^*S\} = \mathcal{O}_{{}^*S}.$$

Se Δ è il gruppo dei valori, chiamiamo Δ_{fin} il sottogruppo convesso di ${}^*\Delta$ generato da $v(k \setminus \{0\})$. Chiamiamo $\dot{\Delta}$ il quoziente ${}^*\Delta/\Delta_{\mathrm{fin}}$ e $\dot{v}$ la relativa valutazione indotta; l'insieme delle $\dot{v}$ verrà chiamato $\dot{S}$. Definiamo analogamente quindi $\mathcal{O}_{\dot{S}}$ e abbiamo naturalmente l'inclusione $\mathcal{O}_{{}^*S} \subset \mathcal{O}_{\dot{S}}$. Abbreviamo per semplicità la notazione a $\mathcal{O}$, ${}^*\mathcal{O}$, $\dot{\mathcal{O}}$ omettendo l'insieme S.

Lemma A.14. *(a) Vale $k = \mathrm{Quot}(\mathcal{O})$ se e soltanto se $\dot{\mathcal{O}} = \mathrm{Quot}_{\mathcal{O}}({}^*\mathcal{O})$.*

(b) Se per ogni $x \in k \setminus \{0\}$ l'insieme S_x dei poli di x è finito, allora per ogni elemento $x \in \dot{\mathcal{O}}$ si ha che ${}^*S_x$ è finito e ${}^*S_x \subset S$.

Dimostrazione. (a) Una valutazione $\dot{v} \in \dot{S}$ è per definizione banale su k, quindi anche su $\mathcal{O}$, cosicché abbiamo automaticamente l'inclusione $\mathrm{Quot}_{\mathcal{O}}({}^*\mathcal{O}) \subset \dot{\mathcal{O}}$.

Se vale l'uguaglianza ogni elemento $\xi \in k \setminus \{0\} \subset \dot{\mathcal{O}}$ appartiene a $\mathrm{Quot}_{\mathcal{O}}({}^*\mathcal{O})$, quindi si scrive come $\xi = a/b$, con $b \in \mathcal{O}$ e $a \in k \cap {}^*\mathcal{O} = \mathcal{O}$. Quindi $k = \mathrm{Quot}(\mathcal{O})$.

Sia invece, in caso di inclusione stretta, $\xi \in \dot{\mathcal{O}}$ con $\xi \notin \mathrm{Quot}_{\mathcal{O}}({}^*\mathcal{O})$. Allora per ogni $b \in \mathcal{O} \setminus \{0\}$ esiste un $v \in {}^*S$ per il quale $v(b\xi) < 0$. Inoltre per ogni numero finito di b_i abbiamo, ponendo $b := \prod_i b_i$, che esiste un v per il quale $v(b\xi) < 0$; in particolare allora

$$0 > v(b\xi) = v(b_1 \cdots b_s \xi) = v(b_1) + \cdots + v(b_i\xi) + \cdots v(b_s) \geq v(b_i\xi),$$

ovvero la relazione $\{(b, v) \mid v(b\xi) < 0\}$ è finitamente soddisfacibile. Esiste allora una soluzione universale $v \in {}^*S$ tale per cui

$$v(b\xi) < 0 \quad \forall b \in \mathcal{O} \setminus \{0\}.$$

Supponiamo che per assurdo sia $k = \mathrm{Quot}(\mathcal{O})$. Allora $v(\xi) \notin \Delta_{\text{fin}}$, poiché altrimenti esisterebbe un $a \in k$ tale per cui $v(a) \leq v(\xi) < 0$ e moltiplicando a per il suo denominatore $b \in \mathcal{O}$ si avrebbe $0 \leq v(b \cdot a) \leq v(b\xi) < 0$. Allora $\dot{v}(\xi) < 0$, contro l'ipotesi che $\xi \in \dot{\mathcal{O}}$.

(b) Se S_x è finito per ogni $x \in k \setminus \{0\}$, allora ${}^*S_x = S_x \subset S$; in particolare allora per ogni $v \in {}^*S \setminus S$ vale $v(k \setminus \{0\}) = 0$. Questo implica in particolare che $\{x \mid v(x) < 0\} = \{x \mid \dot{v}(x) < 0\}$, quindi per ogni $x \in \dot{\mathcal{O}}$ si deve avere ${}^*S_x \subset S$. Se ${}^*S_x$ fosse infinito la relazione $\{(v, v') \mid v \neq v', v \in {}^*S, v' \in {}^*S_x\}$ sarebbe finitamente soddisfacibile e avrebbe soluzione universale in ${}^*S \setminus S$. □

A.4 Sottocampi di ${}^*k$

Sia ora l un sottocampo di ${}^*k$ con grado di trascendenza 1 su k. I valori assoluti $\dot{v} \in \dot{S}$ corrispondono allora a posti di l/k (non banali).

Definizione A.15. *l si dice S-aritmetico se ogni posto non banale di l/k è indotto da un valore assoluto $\dot{v} \in \dot{S}$.*

Definiamo l'anello $\mathcal{O}_l := \dot{\mathcal{O}} \cap l$. Otteniamo immediatamente:

Lemma A.16. *l è S-aritmetico se e soltanto se $\mathcal{O}_l = k$.*

Lemma A.17. *Siano α e β due elementi coprimi rispetto a $\dot{S}$ e supponiamo che valga $(\alpha, \beta) \neq \dot{\mathcal{O}}$. Allora $l_{\alpha/\beta}$ è S-aritmetico.*

Dimostrazione. Poniamo $t := \alpha/\beta$ e supponiamo che l_t non sia S-aritmetico. Esiste allora un posto non indotto da $\dot{S}$; prendiamo l una sottoestensione finita su $k(t)$ sulla quale la restrizione del posto non è indotta da $\dot{S}$. Se tale sottoestensione non esistesse, avremmo $l \cap \dot{\mathcal{O}} = l$ per tutte le sottoestensioni finite, quindi anche $l_t \cap \dot{\mathcal{O}} = l_t$, ovvero anche l_t sarebbe S-aritmetico.

Dato che è possibile costruire un elemento di l che abbia zeri di ordine arbitrariamente grande su qualsiasi numero finito di posti assegnati e polo solamente in un posto dato, e che in $\mathcal{O}_l$ esiste un elemento con almeno un polo, abbiamo che $l = \mathrm{Quot}(\mathcal{O}_l)$. Inoltre essendo l'intersezione di anelli di valutazione discreta $\mathcal{O}_l$ è un dominio di Dedekind. Possiamo allora porre

$$\begin{aligned} \mathfrak{a} &= \{x \in \mathcal{O}_l \mid \dot{v}(x) \geq \max(\dot{v}(t), 0) \quad \forall \dot{v} \in \dot{S}\} \\ \mathfrak{b} &= \{x \in \mathcal{O}_l \mid \dot{v}(x) \geq \max(-\dot{v}(t), 0) \quad \forall \dot{v} \in \dot{S}\}. \end{aligned}$$

Otteniamo $t\mathcal{O}_l = \mathfrak{a} \cdot \mathfrak{b}^{-1}$. Per ipotesi di coprimalità di α e β abbiamo

$$\mathfrak{a} = \alpha\dot{\mathcal{O}} \cap l, \quad \mathfrak{b} = \beta\dot{\mathcal{O}} \cap l$$

mentre per coprimalità di $\mathfrak{a}$ e $\mathfrak{b}$ otteniamo

$$\mathcal{O}_l = \mathfrak{a} + \mathfrak{b} = \alpha\dot{\mathcal{O}} \cap l + \beta\dot{\mathcal{O}} \cap l = (\alpha, \beta) \cap l \ni 1.$$

Quindi $\dot{\mathcal{O}} = (\alpha, \beta)$, contro l'ipotesi. □

Corollario A.18. *Sia $t \in {}^*k \setminus k$ tale che $\{\dot{v} \in \dot{S} \mid \dot{v}(t) < 0\}$ è finito. Se l_t è S-aritmetico allora k è hilbertiano*

Dimostrazione. Se l_t è S-aritmetico allora ogni posto di l_t/k è indotto da un $\dot{v} \in \dot{S}$; in particolare allora i poli di t in $\mathbb{P}(l_t/k)$ sono un insieme finito. Questo significa che il posto all'infinito di $k(t)$ ha un numero finito di estensioni in l_t, dunque per la proposizione A.13 k è hilbertiano. □

A.5 Campi con formula del prodotto

Definizione A.19. k si dice *campo con formula del prodotto su S*, con S insieme di valori assoluti, se valgono le seguenti proprietà:

(a) $S_x = \{v \in S \mid v(x) < 0\}$ è finito per ogni $x \in k \setminus \{0\}$.

(b) $\sum_{v \in S} v(x) = 0$ per ogni $x \in k \setminus \{0\}$.

(c) Esiste un $x \in \setminus\{0\}$ e un $v \in S$ per cui $v(x) \neq 0$.

Lemma A.20. *Sia k un campo con formula del prodotto su S e $t \in {}^*k \setminus k$. Se esiste un $v \in S$ tale per cui $\dot{v}$ sia non banale su $k(t)$, allora l_t è S-aritmetico.*

Dimostrazione. Sia l una sottoestensione di l_t finita su $k(t)$. L'anello $\mathcal{O}_l$ contiene un ideale massimale $\mathfrak{P}_l := \{x \in \mathcal{O}_l \mid \dot{v}(x) > 0\}$ dal quale prendiamo un elemento ξ non nullo. L'insieme dei poli di ξ in ${}^*S$ è finito per il lemma A.14.

Avendo scelto $\xi \in \dot{\mathcal{O}}$, abbiamo che $w(\xi) < 0$ per $w \in {}^*S$ implica $\dot{w}(\xi) = 0$, quindi in particolare $w(\xi) \in \Delta_{\text{fin}}$. Deduciamo allora che

$$\sum_{w(\xi)<0, w \in {}^*S} w(\xi) \in \Delta_{\text{fin}}.$$

Tuttavia vale anche

$$-\sum_{w(\xi)<0, w \in {}^*S} w(\xi) = \sum_{w(\xi)>0, w \in {}^*S} w(\xi) \geq v(\xi).$$

Dato che $\dot{v}(\xi) > 0$, otteniamo $v(\xi) \notin \Delta_{\text{fin}}$; allora il membro di sinistra dell'ultima disuguaglianza non appartiene a Δ_{fin}. Assurdo. □

Teorema A.21. *I campi con formula del prodotto sono hilbertiani.*

Dimostrazione. Sia $x \in k \setminus \{0\}$ e $v \in S$ tale per cui $v(x) \neq 0$. Prendiamo un elemento $\omega \in {}^*\mathbb{N} \setminus \mathbb{N}$ e fissiamo $t := x^\omega$. I poli di t in ${}^*S$ sono gli stessi di x, in quanto S_x è un insieme finito. Vale $v(t) = \omega \cdot v(x)$, quindi $\dot{v}(t) \neq 0$. Possiamo allora applicare il lemma A.20 e ottenere un l_t S-aritmetico. Per il corollario A.18 k è hilbertiano. □

A.6 Estensioni algebriche

Consideriamo ora un'estensione K/k algebrica, possibilmente infinita. In generale l'ingrandimento ${}^*K/{}^*k$ non sarà un'estensione algebrica, ma solamente sotto opportune condizioni. Definiamo:

$$\dot{k} := {}^*k \cdot K,$$
$$\dot{K} := \overline{{}^*k} \cap {}^*K.$$

L'estensione $\dot{K}/\dot{k}$ è algebrica.

Definizione A.22. Un'estensione K/k algebrica si dice di *tipo finito* se per ogni $n \in \mathbb{N}$ l'insieme $L_n(K/k) := \{L \mid k \subset L \subset K, [L : k] \leq n\}$ è finito.

Lemma A.23. *L'estensione $\dot{K}/\dot{k}$ è banale se e soltanto se K/k è di tipo finito.*

Dimostrazione. Notiamo che $L_n(K/k)$ è definito al prim'ordine come

$$\begin{aligned} L_n(K/k) \quad = \quad & \{L \in \mathscr{P}(K) \mid L \text{ campo } \vee \\ & \forall x \in L \exists c_0, \ldots, c_{n-1} \in k \; x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0\} \end{aligned}$$

quindi

$$\begin{aligned} {}^*L_n(K/k) \quad = \quad & \{L \in {}^*\mathscr{P}(K) \mid L \text{ campo } \vee \\ & \forall x \in L \; \exists c_0, \ldots, c_{n-1} \in {}^*k \\ & x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0\} \subset Ł_n({}^*K/{}^*k). \end{aligned}$$

Se però consideriamo un'estensione $L/{}^*k$ con $[L : {}^*k] \leq n$, prendendone un generatore α abbiamo

$$L = \{x \in {}^*K \mid \exists c_1, \ldots, c_n \in {}^*k \; x = c_1 + \cdots + c_n\alpha^n\}.$$

L'insieme L è allora interno, ossia $L \in {}^*\mathscr{P}(K)$, quindi ${}^*L_n(K/k) = L_n({}^*K/{}^*k)$. In virtù di questa affermazione l'ipotesi sul tipo finito implica $L_n(K/k) = L_n({}^*K/{}^*k)$. Abbiamo ${}^*L = {}^*(k(\alpha)) = {}^*k(\alpha) = {}^*k \cdot L$, quindi ogni estensione algebrica finita di ${}^*k$ contenuta in ${}^*K$ è composizione di un'estensione algebrica di k contenuta in K e di ${}^*k$. In particolare allora $\dot{K} = {}^*k\dot{K} = \dot{k}$.

Se invece K/k non è di tipo finito esiste almeno un'estensione L di grado finito che non è composto di ${}^*k$ e di un'estensione finita di k; allora $L \not\subseteq {}^*k \cdot K$, quindi $\dot{k} \neq \dot{K}$. □

Supponiamo ora di avere K/k di Galois, con gruppo profinito Γ. Sia Δ un gruppo di automorfismi di K finito.

Definizione A.24. K/k si dice Δ-*estensione* se

(a) Il campo K^Δ è Γ-invariante.

(b) k è Δ-invariante e $[k : k^\Delta] = |\Delta|$.

Lemma A.25. *Sia K/k una Δ-estensione.*

(a) Se l è una sottoestensione normale, allora K/l e l/k sono Δ-estensioni.

(b) Se l è un sottocampo di k algebricamente chiuso in k sul quale Δ agisce fedelmente, e L la chiusura algebrica di l in K, allora L/l è una Δ-estensione.

Dimostrazione. (a) Ovviamente l è Δ-invariante, per ipotesi di normalità di l/k; inoltre $l^\Delta \cap k \subset K^\Delta \cap k$, ma $K^\Delta \cap k = k^\Delta$ per confronto dei gradi, quindi $l^\Delta \cap k = k^\Delta$. In particolare allora $[l : l^\Delta] = [k : k^\Delta] = |\Delta|$. Infine $l^\Delta = l \cap K^\Delta$ è ovviamente Γ-invariante, mentre k^Δ è invariante per l'azione di $\mathrm{Gal}(l/k)$ in quanto restrizione dell'azione di Γ.

(b) Abbiamo immediatamente $[l : l^\Delta] = |\Delta|$. Inoltre $\Delta(\bar{l} \cap K) = \overline{\Delta(l)} \cap K = \bar{l} \cap K$, quindi L è Δ-invariante. Infine $L^\Delta = L \cap K^\Delta$ è Γ-invariante, quindi anche $\mathrm{Gal}(L/l)$ invariante in quanto restrizione dell'azione di Γ. □

Proposizione A.26. *Se K/k è una Δ-estensione, tale è anche $\dot{K}/\dot{k}$.*

Dimostrazione. Notiamo che se $l \in L_n(K/k)$, allora la chiusura normale $\tilde{l}$ di l appartiene a $\tilde{l} \in L_{n!}(K/k)$; quest'affermazione è esprimibile al primo ordine, quindi è vera anche in ${}^*K$, da cui ricaviamo che $\dot{K}/\dot{k}$ è di Galois. L'azione di Δ si estende naturalmente a ${}^*K$, quindi a $\dot{K}$; essendo l'azione di Δ fedele su k, lo è anche su ${}^*k$, quindi $[\dot{k} : \dot{k}^\Delta] = |\Delta|$. □

A.7 Elementi hilbertiani

Estendiamo la notazione l_t al caso di un vettore $\mathbf{t} = (t_1, \ldots, t_n)$ di elementi di ${}^*k$ definendo $l_\mathbf{t} := \overline{k(t_1, \ldots, t_n)} \cap {}^*k$.

Definizione A.27. $\mathbf{t}$ si chiama *sistema hilbertiano* (di lunghezza n) per ${}^*k$ se $t_1, \ldots, t_n$ sono algebricamente indipendenti su k e se $l_\mathbf{t} = k(\mathbf{t})$.

Proposizione A.28. *Un campo k è hilbertiano se e soltanto se in ${}^*k$ esistono sistemi hilbertiani di qualsiasi lunghezza $n \in \mathbb{N} \setminus \{0\}$.*

Dimostrazione. Se esiste un sistema hilbertiano $\mathbf{t}$, il campo $k(\mathbf{t})$ ha una formula del prodotto, quindi è hilbertiano, mentre è algebricamente chiuso in ${}^*k$; applicando la proposizione A.11 otteniamo che k è hilbertiano.

Viceversa supponiamo k hilbertiano. Sappiamo ora dalla proposizione A.10 che esiste un sistema hilbertiano di lunghezza 1. Procediamo ora per induzione e supponiamo che esista un $\mathbf{t} = (t_1, \ldots, t_{n-1})$ sistema hilbertiano in ${}^*k$. Prendiamo un ulteriore ingrandimento ${}^+$ di ${}^*k$; dato che ${}^*k$ è hilbertiano per trasferimento da k, esiste un elemento $t_n \in {}^+({}^*k) \setminus {}^*k$ per cui ${}^*k(t_n)$ è algebricamente chiuso in ${}^+({}^*k)$. Dato che $k(\mathbf{t})$ è algebricamente chiuso in ${}^*k$,

$k(\mathbf{t}, t_n)$ è algebricamente chiuso in ${}^*k(t_n)$ e quindi anche in ${}^+({}^*k)$. Il sistema $\mathbf{t}' := (t_1, \ldots, t_n)$ è quindi hilbertiano in ${}^+({}^*k)$.

La relazione

$$R = \{((f, \mathbf{t}), \mathbf{t}') \mid f(\mathbf{t}, X), f(\mathbf{t}', X) \text{ irriducibili e } \mathbf{t} \neq \mathbf{t}'\}$$

ristretta agli $f \in k[T_1, \ldots, T_n, X]$ irriducibili ha quindi soluzione universale in ${}^+({}^*k)$. La formula

$$\exists \mathbf{t} : \bigvee_{i=1}^{s} (R((f, \mathbf{t}_i), \mathbf{t}) \vee \mathbf{t} \neq \mathbf{t}_i)$$

è allora verificata in ${}^+({}^*k)$, quindi anche in k, per ogni scelta fissata di un numero finito di $\mathbf{t}_i \in k^n$; ne consegue che R è finitamente soddisfacibile ed ha pertanto soluzione universale anche in ${}^*k$. □

Lemma A.29. *Sia K/k un'estensione qualsiasi. Se $\mathbf{t}$ è un sistema hilbertiano per ${}^*K$ le cui componenti appartengono a ${}^*k \setminus k$, allora è anche un sistema hilbertiano per ${}^*k$.*

Dimostrazione. Dato che per ogni $x \in K$ la formula $x \notin k$ deve restare vera in ${}^*K$, deduciamo che ${}^*k \cap K = k$. Allora $l_{\mathbf{t}} = \overline{k(\mathbf{t})} \cap {}^*k \subset \overline{K(\mathbf{t})} \cap {}^*k \subset K(t) \cap {}^*k = k(\mathbf{t})$. □

Lemma A.30. *Sia K/k un'estensione algebrica di tipo finito. Allora ogni sistema hilbertiano $\mathbf{t}$ per k lo è anche per K. Inoltre se k è hilbertiano lo è anche K.*

Dimostrazione. Dall'ipotesi che $\mathbf{t}$ è un sistema hilbertiano per k otteniamo

$$\begin{aligned} \overline{k(\mathbf{t})} \cap {}^*k &= k(\mathbf{t}) \\ K \cdot (\overline{k(\mathbf{t})} \cap {}^*k) &= K \cdot k(\mathbf{t}) = K(\mathbf{t}) \\ (K \cdot \overline{k(\mathbf{t})}) \cap \dot{k} &= K(\mathbf{t}) \\ \overline{K(\mathbf{t})} \cap \dot{k} &= K(\mathbf{t}). \end{aligned}$$

D'altra parte $\dot{k} = \dot{K}$ per il lemma A.23 $\dot{K} = \dot{k}$, quindi

$$\overline{K(\mathbf{t})} \cap {}^*K = \overline{K(\mathbf{t})} \cap \dot{K} = \overline{K(\mathbf{t})} \cap \dot{k} = K(\mathbf{t}).$$

Per la proposizione A.28 quando k è hilbertiano possiede un sistema hilbertiano, e tale resta per K, quindi anche K è hilbertiano. □

Lemma A.31. *Sia K/k una Δ-estensione con un sistema hilbertiano $\mathbf{t}$ per ${}^*k$. Se $\mathbf{t}$ è Δ-invariante, allora $l_{\mathbf{t}}/K(\mathbf{t})$ è una Δ-estensione.*

Dimostrazione. Dalla dimostrazione del lemma precedente ricaviamo che $l_{\mathbf{t}} \subset \dot{K}$, mentre $K(\mathbf{t}) \subset \dot{k}$, con $K(\mathbf{t})$ algebricamente chiuso in $\dot{k}$. Per la proposizione A.26 $\dot{K}/\dot{k}$ è una Δ-estensione, mentre Δ agisce fedelmente su $K(\mathbf{t})$ per ipotesi di invarianza di $\mathbf{t}$; quindi possiamo applicare il lemma A.25(b) e ottenere che $l_{\mathbf{t}}/K(\mathbf{t})$ è una Δ-estensione. □

Proposizione A.32. *Sia K/k una Δ-estensione. Se esiste un sistema hilbertiano Δ-invariante per ${}^*k$ di lunghezza maggiore di 1 e $\Delta \neq \{e\}$, allora K è hilbertiano.*

Dimostrazione. Sia $\mathbf{t}$ un sistema hilbertiano Δ-invariante di ${}^*k$. L'estensione $l_{\mathbf{t}}/K(\mathbf{t})$ è allora una Δ-estensione per il lemma A.31.

Per qualsiasi scelta di $c_i \in k$ non tutti nulli, l'elemento $t := c_1t_1 + \cdots + c_nt_n$ è hilbertiano, poiché $k(t)$ è algebricamente chiuso in $k(\mathbf{t})$. Lo stesso vale per $K(t)$.

Osserviamo ora che $l_t \cdot K(\mathbf{t})$ è una sottoestensione normale su $K(\mathbf{t})$ di $l_{\mathbf{t}}$, quindi per il lemma A.25(a) Δ agisce su $l_t \cdot K(\mathbf{t})$. Se però δ è un elemento non banale, possiamo facilmente costruire un t tale per cui $t^\delta/t \notin K$. Notiamo allora che t^δ e t sono algebricamente indipendenti su K, quindi $l_{t^\delta} \cap l_t = K$. Deduciamo allora che

$$K(\mathbf{t}) = l_{t^\delta} \cdot K(\mathbf{t}) \cap l_t \cdot K(\mathbf{t}) = l_t \cdot K(\mathbf{t}).$$

Dato che $K(t)$ è algebricamente chiuso in $K(\mathbf{t})$ otteniamo allora $l_t = K(t)$. □

Teorema A.33 (Weissauer)**.** *Se K/k è un'estensione algebrica di un campo hilbertiano k, allora ogni estensione finita propria di K è hilbertiana.*

Dimostrazione. Sia L/K un'estensione finita propria. Scegliamo allora un elemento α tale per cui $l := k(\alpha)$ è normale su k e $l \cdot K \supset L$. Il gruppo $\Delta := \mathrm{Gal}(l/k)$ ci permette di applicare la proposizione A.32 e ottenere che $l \cdot K$ ha un sistema hilbertiano. D'altra parte nella dimostrazione della proposizione A.32 abbiamo scelto t in modo che fosse $t^\delta/t \notin l \cdot K$; siamo allora liberi di scegliere t in qualunque sottoestensione di $l \cdot K$ diversa da K, in particolare in L. Per il lemma A.29 otteniamo allora che anche L è hilbertiano. □

Bibliografia

[1] Emil Artin, *Algebraic numbers and algebraic functions*, AMS Chelsea Publishing, Providence, RI, 2006, Reprint of the 1967 original. MR MR2218376 (2006k:11001)

[2] Otto Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics, vol. 81, Springer-Verlag, New York, 1981, Translated from the German by Bruce Gilligan. MR MR648106 (83d:30046)

[3] Kurt Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), no. 2-3, 289–307. MR MR707048 (84m:12023)

[4] Jürgen Klüners and Gunter Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J. Symbolic Comput. **30** (2000), no. 6, 675–716, Algorithmic methods in Galois theory. MR MR1800033 (2001i:12005)

[5] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999. MR MR1711577 (2000k:12004)

[6] Peter Roquette, *Nonstandard aspects of Hilbert's irreducibility theorem*, Model theory and algebra (A memorial tribute to Abraham Robinson), Springer, Berlin, 1975, pp. 231–275. Lecture Notes in Math., Vol. 498. MR MR0401771 (53 #5598)

[7] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996. MR MR0327712 (48 #6054)

[8] K. D. Stroyan and W. A. J. Luxemburg, *Introduction to the theory of infinitesimals*, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976, Pure and Applied Mathematics, No. 72. MR MR0491163 (58 #10429)

[9] Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction. MR MR1405612 (98b:12003)

[10] Rainer Weissauer, *Der Hilbertsche Irreduzibilitätssatz*, J. Reine Angew. Math. **334** (1982), 203–220. MR MR667458 (84c:12020)